

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

DİJİTAL DÜNYADA SİBER GÜVENLİK DAVRANIŞI

AHMET DÜZENCİ

DOKTORA TEZİ
İŞLETME ANABİLİM DALI

DANIŞMAN: PROF. DR. HAKAN KİTAPÇI

ŞUBAT 2024

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

DİJİTAL DÜNYADA SİBER GÜVENLİK DAVRANIŞI

AHMET DÜZENÇİ

DOKTORA TEZİ
İŞLETME ANABİLİM DALI

DANIŞMAN: PROF. DR. HAKAN KİTAPÇI

ŞUBAT 2024

DOKTORA JÜRİ ONAY FORMU

GTÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun 22/01/2024 tarih ve 2024/07 sayılı kararıyla oluşturulan jüri tarafından 14/02/2024 tarihinde tez savunma sınavı yapılan Ahmet Düzençi'nin tez çalışması İşletme Anabilim Dalında DOKTORA tezi olarak kabul edilmiştir.

JÜRİ

ÜYE
(TEZ DANIŞMANI) : PROF.DR. HAKAN KİTAPÇI

ÜYE : PROF.DR. MEHMET ŞAHİN GÖK

ÜYE : PROF.DR. AYŞE GÜNSEL

ÜYE : DOÇ.DR. SERHAT ERAT

ÜYE : PROF.DR. ERKUT ALTINDAĞ

ONAY

Gebze Teknik Üniversitesi Lisansüstü Eğitim Enstitüsü Yönetim Kurulunun
...../...../..... tarih ve/..... sayılı kararı.

Sevgili Eşim Didem'e, Değerli Oğlum Ali Tuğrul'a ve Sevgi Dolu Aileme;

*Sizlerin sevgi, destek ve ilhamıyla tamamladığım bu tez,
birlikte geçirdiğimiz her anın bana kattığı değeri yansıtmaktadır.
Sizinle birlikte gelişmek ve öğrenmek benim için büyük bir ayrıcalıktır.*

Sonsuz sevgi ve teşekkürlerimi sunarım.

ÖZET

İletişim ağlarına yönelik artan siber saldırılar, insanlık için önemli güvenlik tehditlerinden biri olarak ön plana çıkmaktadır. Bu tür saldırılar hassas verileri ve kritik altyapıları riske atmakla birlikte, aynı zamanda ulusal güvenlik ve küresel ekonomi için de büyük riskler oluşturmaktadır. Teknolojinin ilerlemesiyle birlikte, bireyler, kurumlar ve devletler arasında bütüncül bir siber güvenlik anlayışı oluşturmanın önemi artmıştır. Siber saldırıların etkilerini azaltmak için gelişmiş teknolojik çözümleri, bireylerin günlük siber güvenlik uygulamalarıyla birleştirmek zorunludur. Son teknoloji siber güvenlik çözümleri ile insanın doğru eylemlerinin iş birliği, dijital ekosistemimizin genel dayanıklılığını artırarak çok katmanlı bir savunma oluşturabilir. Bu bütünlük yaklaşım, siber tehditlere karşı bir adım önde olma çabamızda, dijital dünyamızın güvenliğini sağlamak için temel bir gerekliliktir.

Bu tez çalışması, bireylerin karar verme tarzlarının siber güvenlik uyum davranışını ne ölçüde etkilediğini incelemeye odaklanmaktadır. Tez çalışması kapsamında, koruma motivasyonu teorisi ilkelerine dayalı bir kavramsal model geliştirilmiş ve bu model, çalışanlar ve iş deneyimi olan öğrencilerin anket sonuçlarından oluşan bir veri seti ile test edilmiştir. Bireylerin karar verme tarzlarının siber güvenlik uyum davranışları üzerinde belirgin bir etkisi olduğunu ve bu etkilerin, bireylerin farklı karar verme yaklaşımlarına bağlı olarak önemli farklılıklar gösterdiğini ortaya koymaktadır. Ayrıca çalışma bulguları, siber güvenlik uyum davranışını etkileyen önemli bir başka faktör olan güvenlik farkındalığının da önemini vurgulamaktadır. Bu araştırma, bireylerin karar verme tarzlarının siber güvenlik uyum davranışını etkileyen mekanizmaları anlamamıza yeni bakış açıları sunmaktadır. Çalışma bulguları, bireylerin siber güvenlik uyum davranışını etkileyen mekanizmaları kavramamız bakımından yeni perspektifler sunmakta ve böylece, siber güvenliğin sağlanması için bireysel farklılıkları da dikkate alana kapsayıcı organizasyonel planları ortaya koymayı mümkün kılmaktadır.

Anahtar Kelimeler: Siber Güvenlik Uyum Davranışı, Karar Verme Tarzı, Koruma Motivasyonu Teorisi, Güvenlik Farkındalığı.

ABSTRACT

The escalating frequency of assaults on vital communication networks represents a major security concern for humanity. These attacks not only jeopardize sensitive data and critical infrastructure but also pose significant risks to national security and the global economy. As technology advances, it becomes crucial to foster a collective cybersecurity mindset among individuals, organizations, and governments. To mitigate the impact of these assaults, it is imperative to integrate advanced technological safeguards with the practical cybersecurity practices of individuals. The collaboration between cutting-edge cybersecurity technologies and human vigilance can create a multi-layered defense that strengthens the overall resilience of our digital ecosystems. This combined approach is essential in ensuring the safety of our interconnected world, as we strive to stay one step ahead of cyber threats.

In this dissertation, our focus centers on investigating how individual approaches to decision-making impact behaviors related to cybersecurity compliance. In order to achieve this, a conceptual framework grounded on the principles of protection motivation theory is developed and subjected to testing, utilizing a dataset that included responses from individuals, including those with real-world work experience, such as employees and students. Statistical analyses involving regression techniques are conducted to assess the influence of individual decision-making styles on the adoption of cybersecurity compliance practices. Findings demonstrate that personal styles in decision-making have a discernible effect on their cybersecurity compliance behaviors, with these impacts exhibiting notable variations based on distinct decision-making approaches. Additionally, this dissertation underscores the pivotal role of security awareness as a key factor influencing cybersecurity compliance. The study findings offer new perspectives in terms of understanding the mechanisms that affect individuals' cybersecurity compliance behavior, thus making it possible to put forward comprehensive organizational plans that take into account individual differences to ensure cybersecurity.

Keywords: Cybersecurity Compliance Behavior, Decision-Making Style, Protection Motivation Theory, Security Awareness.

TEŞEKKÜR

Öğrenim ve tez sürecim boyunca desteğini her zaman hissettiğim saygıdeğer danışmanım Prof. Dr. Hakan KİTAPÇI'ya teşekkürlerimi sunuyorum. Değerli hocam Prof. Dr. Mehmet Şahin GÖK'e, kıymetli rehberlikleri ve destekleri için çok teşekkür ederim. Tez izleme sürecimde değerli fikirleri ile destek sunan Prof. Dr. Ayşe GÜNSEL'e ve tez savunmamdaki önerileriyle bana yol gösteren Prof. Dr. Erkut ALTINDAĞ ve Doç. Dr. Serhat ERAT hocalarıma teşekkür ederim.

Bu süreçteki destekleri ve sabrı için sevgili eşim Didem DÜZENCI'ye ve kıymetli oğlum Ali Tuğrul DÜZENCI'ye içten teşekkürlerimi sunarım. Sizlerin varlığı ve destekleri, benim için her şeyden önemliydi.

Aileme, babam Haydar DÜZENCI'ye, annem Hasibe DÜZENCI'ye, ablalarım Meltem DANIŞMAN'a ve Mehtap KARAKAYA'ya, sonsuz şükranlarımı iletmek isterim. Sizlerin sürekli desteği ve teşvikleri, bu tezin yazım sürecinde benim için büyük bir motivasyon kaynağı oldu.

Eşim sayesinde edindiğim annem Fahriye ÖZCAN'a ve babam Galip ÖZCAN'a içtenlikle verdikleri destek için teşekkür etmek isterim.

Doktora sürecimde edindiğim kıymetli dostlarım Nilşah ÇAVDAR AKSOY'a ve Nihal YAZICI'ya ders sürecimizdeki samimi arkadaşlıkları ve veri toplama aşamasındaki destekleri için teşekkür ederim.

İÇİNDEKİLER

	<u>Sayfa</u>
ÖZET	ii
ABSTRACT	iii
TEŞEKKÜR	iv
İÇİNDEKİLER	v
SİMGELER ve KISALTMALAR DİZİNİ	vi
ŞEKİLLER DİZİNİ	vii
TABLolar DİZİNİ	viii
1. GİRİŞ	1
1.1. Tezin Araştırma Sorusu ve Amaçları	1
1.2. Tezin Önemi	2
1.3. Tezin Ana Hatları	2
2. TEORİK GEÇMİŞ	4
2.1. Karar Verme Tarzları	4
2.2. Siber Güvenlik Uyum Davranışı ve Koruma Motivasyonu Teorisi	10
2.3. Kavramsal Model	14
2.4. Hipotez Geliştirme	15
2.4.1. Siber Güvenlik Uyum Davranışı ve Algılanan Önem Derecesi	16
2.4.2. Siber Güvenlik Uyum Davranışı ve Algılanan Önem Derecesi	17
Algılanan Savunmasızlık	
2.4.3. Siber Güvenlik Uyum Davranışı ve Algılanan Öz Yeterlik	18
2.4.4. Siber Güvenlik Uyum Davranışı ve Yanıt Etkinliği	19
2.4.5. Siber Güvenlik Uyum Davranışı ve Algılanan Engel	20
2.4.6. Siber Güvenlik Uyum Davranışı ve Güvenlik Farkındalığı	20
3. YÖNTEM	23
3.1. Ölçekler	23
3.2. Verilerin Toplanması ve Örneklem Prosedürü	24
3.3. Veri Analizi	27
4. BULGULAR	30
5. ARAŞTIRMA SONUÇLARININ YORUMLANMASI	36
5.1. Teorik Katkıları	39
5.2. Uygulamaya Yönelik Çıkarımlar	39
5.3. Araştırmanın Kısıtları ve Gelecek Araştırmalar İçin Öneriler	40
6. SONUÇ	42
KAYNAKLAR	44
ÖZGEÇMİŞ	53
TEZ METNİNDEN TÜRETİLEN YAYINLAR/SUNUMLAR	54
EKLER	55

SİMGELER ve KISALTMALAR DİZİNİ

KMT	:	Koruma Motivasyonu Teorisi
KVT	:	Karar Verme Tarzları
SGUD	:	Siber Güvenlik Uyum Davranışı
GKVT	:	Genel Karar Verme Tarzı Envanteri



ŞEKİLLER DİZİNİ

Şekil 2.1: Kavramsal Model.

Sayfa
15



TABLÖLAR DİZİNİ

	<u>Sayfa</u>
Tablo 3.1: Örneklemin Demografik Yapısı.	26
Tablo 3.2: Faktör Analizi Sonuçları.	28
Tablo 4.1: Korelasyonlar.	30
Tablo 4.2: Genel Regresyon Analizi Sonuçları.	31
Tablo 4.3: Rasyonel Karar Verme Tarzına Sahip Bireyler İçin Regresyon Analizi Sonuçları.	32
Tablo 4.4: Sezgisel Karar Verme Tarzına Sahip Bireyler İçin Regresyon Analizi Sonuçları.	33
Tablo 4.5: Bağımlı Karar Verme Tarzına Sahip Bireyler İçin Regresyon Analizi Sonuçları.	34
Tablo 4.6: Regresyon Analizleri Özeti.	35

1. GİRİŞ

Siber güvenlik harcamaları kurumların bütçelerinde giderek daha fazla yük oluşturmalarına rağmen, siber saldırıların devam etmesi önemli bir sorun olarak güncelliğini korumaktadır. Cybersecurity Ventures (2021) tarafından bildirildiği üzere, siber güvenlik ürün ve hizmetlerine yönelik küresel harcamaların 2021'den 2025'e kadar yıllık %15 oranında artarak toplam 1,75 trilyon dolara ulaşacağı öngörülmektedir. Siber güvenliğe ayrılan bütçenin artmasıyla birlikte, siber saldırıların sıklığı ve karmaşıklığı da artmakta ve insan hatası, veri ihlallerinin temel nedeni olmaya devam etmektedir. Verizon (2022) tarafından yayınlanan 2022 Veri İhlal Araştırmaları Raporu, doğrulanan veri ihlallerinin %82'sinin çalıntı kimlik bilgileri, kimlik avı ve kötüye kullanım gibi insan odaklı tekniklerden kaynaklandığını ortaya koymakta ve siber güvenlikte insan faktörlerinin merkezi rolünün altını çizmektedir. Teknolojik çözümler, insan hatalarından kaynaklanan siber olayların azaltılmasına katkı sağlarken, bunların tamamen önlenmesinin henüz mümkün olmadığı görülmektedir. Sonuç olarak, teknik önlemlerin siber güvenlik uyum davranışlarıyla tamamlanması vazgeçilmez hale gelmekte ve bu da bireylerin siber güvenliği sağlamak için kuruluşları tarafından bildirilen güvenlik protokollerine uymasını gerektirmektedir.

1.1. Tezin Araştırma Sorusu ve Amaçları

Bireylerin siber güvenliğe uyum davranışlarını açıklamak için çeşitli teorik çerçevelerden yararlanılarak çok sayıda araştırma yapılmıştır. Örneğin; rasyonel seçim teorisi (örneğin Vance ve Siponen, 2012; Bulgurcu vd., 2010; Han vd., 2017; Hu vd., 2011), planlı davranış teorisi (örneğin Hazari vd., 2008; Herath ve Rao, 2009a; Bulgurcu vd., 2010; Ifinedo, 2014; Moody vd., 2018), genel caydırıcılık teorisi (örneğin Lee vd., 2004; Chen vd., 2012; Kankanhalli vd., 2003; Moody vd., 2018; Siponen ve Vance, 2010; Siponen vd., 2007), nötralizasyon teorisi (örneğin Barlow vd., 2013; Siponen ve Vance, 2010) ve koruma motivasyonu teorisi (örneğin Vance vd., 2012; Crossler ve Bélanger, 2014; Siponen ve Vance, 2014; Safa vd., 2015; Li vd., 2019). Bununla birlikte, bu çalışmaların çoğu ağırlıklı olarak algılanan maliyet (Boss vd., 2015), algılanan etkinlik (Herath ve Rao, 2009b) ve algılanan duyarlılık

(Warkentin vd., 2016) dâhil olmak üzere algıyla ilişkili yönler odaklanmıştır. Bunların yanı sıra, araştırmaların öznel normlar (Hadlington, 2017; Ifinedo, 2014; Anderson ve Agarwal, 2010; Herath ve Rao, 2009a, 2009b), sosyal etki (Tu vd., 2015) ve ödüller (Siponen vd., 2014; Boss vd., 2009) gibi dış etkiler üzerinde yoğunlaştığı da gözlemlenmektedir. Her ne kadar algılanan ve dışsal faktörlere vurgu yapılsa da (Lu, 2018), söz konusu davranışın açıklanmasında bireylerin karar verme tarzları gibi içsel yönlerine yeterince dikkat edilmediği görülmektedir (Egelman ve Peer, 2015; Gratian vd., 2018; Donalds ve Osei-Bryson, 2020). Bu tez, içsel faktörlerden biri olan bireylerin karar verme tarzlarının siber güvenlik uyum davranışı üzerindeki etkisini araştırmaktadır. Bu bakımdan, temel araştırma sorusu şu şekilde belirlenmiştir: "Farklı karar verme tarzlarına sahip çalışanlar siber güvenlik uyum davranışları açısından ne ölçüde farklılık gösterir?".

1.2. Tezin Önemi

Yukarıda bahsedilen araştırma boşluğundan hareketle, Koruma Motivasyonu Teorisine (KMT) (Rogers, 1975, 1983) dayanan kavramsal bir model ortaya koyulmuş ve bu model ampirik teste tabi tutulmuştur. Bulgular, bireylerin siber güvenlik uyum davranışlarının anlaşılmasına yönelik yeni bilgiler sunarak mevcut literatüre önemli katkılar sağlamaktadır. Ayrıca tezin bulguları, farklı karar alma mekanizmalarına sahip bireylerin siber güvenlik uyum davranışlarında farklılıklar olduğunu gösteren sınırlı çalışmaların (Egelman ve Peer, 2015; Gratian vd., 2018; Donalds ve Osei-Bryson, 2020) sonuçlarıyla da uyumludur. Ayrıca bu tez, yalnızca davranışsal niyetlere odaklanmak yerine, bireylerin gerçekleştirdiği gerçek siber güvenlik koruyucu eylemlerini analiz etmektedir. Bunu yapılmasındaki hedef, bireysel karar alma süreçlerine dayanan daha pratik ve gerçekçi uygulamalar sağlayarak siber güvenliğin nasıl geliştirilebileceğini aydınlatmaktır.

1.3. Tezin Ana Hatları

Bu tez altı bölümden oluşmaktadır;

2. bölümde, ilgili literatür gözden geçirilmekte ve tezin teorik temelleri açıklanmakta olup kavramsal model çerçevesinde oluşturulan öngörüler açıklanmaktadır.

3. bölümde, bu tezde kullanılan metodoloji ayrıntılı olarak ele alınmakta ve ‘Ölçekler’, ‘Verilerin Toplanması ve Örnekleme Prosedürü’ ve ‘Veri Analizi’ bölümlerine ilişkin kapsamlı bilgiler sunulmaktadır.

4. bölümde, analizin sonuçları açıklanmakta ve çalışmadan elde edilen temel bulgulara ışık tutulmaktadır.

5. bölümde, araştırma soruları çerçevesinde kapsamlı bir tartışma yürütülmektedir. Bu bölüm ‘Teorik Katkılar’, ‘Uygulamaya Yönelik Katkılar’ ve ‘Araştırmanın Kısıtları ve Önerileri’ bölümlerini kapsamaktadır.

6. bölümde, tez temel bulguları özetleyen bir sonuç sunumuyla özetlemektedir.



2. TEORİK GEÇMİŞ

Teorik geçmiş bölümü, bu çalışmanın kavramsal temelini oluşturmaktadır. Bu kapsamda, bölümde temel olarak iki önemli alan incelenmektedir. Bunlar; “Karar Verme Tarzları (KVT)” ve “Siber Güvenlik Uyum Davranışı (SGUD) ve Koruma Motivasyonu Teorisi (KMT)”.

Karar verme tarzları, bireylerin karar verme anlarına geldiklerinde kullandıkları çeşitli bilişsel yaklaşımları kapsar ve onların tercihleri ve alışılmış karar verme modları hakkında fikir verir. Teorik çerçevelerin incelenmesi kapsamında, karar verme tarzlarının genel yaklaşımı açıklanmaktadır. Sonrasında Siber Güvenlik Uyum Davranışı (SGUD) alanına giriş yapılarak, bireylerin siber güvenlik önlemlerine bağlılığı ve Koruma Motivasyonu Teorisi (KMT) kapsamındaki dinamikleri incelenmektedir. Bu bağlamda, siber güvenlik uyumluluğunu etkileyen karmaşık dinamikleri yapısal olarak temsil eden kavramsal model ortaya konulmaktadır. Daha sonra, mevcut teorilere dayalı olarak test edilebilir önermeleri dile getirdiğimiz hipotez geliştirme bölümüne geçilmektedir.

Bölüm, alt bölümleri ile birlikte literatürün kapsamlı bir incelemesini oluşturmakta ve daha sonraki ampirik araştırmamızın kavramsal temelini oluşturmaktadır.

2.1. Karar Verme Tarzları

Davranış bilimleri alanındaki araştırmacılar, insanların karşılaştırılabilir durumlarda genellikle zaman içinde geliştirdikleri alışkanlıklar tarafından yönlendirilen tipik tepkiler sergileme eğiliminde olduklarını ileri sürmektedir (Driver, 1979; Scott ve Bruce, 1995; Thunholm, 2004). Bireylerin karar verme süreçlerinde sergiledikleri bu tekrarlanan ve karakteristik tepkilere, bilimsel literatürde “Karar Verme Tarzları” adı verilmektedir (Rowe ve Mason, 1987; Scott ve Bruce, 1995; Thunholm, 2004).

Karar verme durumlarıyla karşı karşıya kaldıklarında bireyler, çeşitli bilgi kaynaklarının entegrasyonunu içeren çok yönlü bir sürece dâhil olurlar. Bu karmaşık görev, çeşitli faktörlerin dikkate alınmasını, alternatiflerin tartılmasını ve uygun bir seçime ulaşmak için strateji oluşturulmasını gerektirir. Karar verme sürecimiz, doğası

gereği benzersiz deneyimlerimiz ve çevremizdeki dünya hakkında edindiğimiz bilgilerle şekillenir.

Bilişsel stiller ve karar verme tarzları birbiriyle yakından ilişkili kavramlardır. Aslında "bilişsel stiller" ve "karar verme tarzları" terimleri sıklıkla birbirinin yerine kullanılmaktadır (Bavolar ve Orosova, 2015). Bazı durumlarda, başlangıçta bilişsel stilleri değerlendirmek için tasarlanan araçlar, karar verme tarzlarını değerlendirmek için sıklıkla kullanılmaktadır (Appelt vd., 2011).

Genellikle bireyin bilgiyi ele alma ve sorunları çözmede tercih ettiği yöntem olarak görülen bilişsel tarz (Messick ve Fritzky, 1963), karar verme uygulamalarını şekillendirmede çok önemli bir rol oynar. Karar verme tarzı ile bilişsel stil arasındaki bu bağlantı, bireylerin karmaşık seçimlerde nasıl ilerlediğini anlamanın temelini oluşturur.

Karar vermede bilişsel tarz terimi tipik olarak bireyin karar süreçlerinin nasıl ortaya çıktığını anlamak için gerekli olan temel "düşünme uygulamalarını" ifade eder. Literatürde karar verme tarzları, bilişsel stillerin bir alt bileşeni olarak tanımlanmaktadır (Hunt vd., 1989; Kozhevnikov, 2007).

Bilişsel stil ile karar verme tarzı arasındaki etkileşimi anlamak, bireylerin kararlara neden belirli şekillerde yaklaşma eğiliminde olduklarına ışık tutar. Bilişsel stillerimize derinlemesine yerleşmiş olan düşünme uygulamalarımızın, yalnızca bilgiyi nasıl işlediğimizi değil aynı zamanda bu bilişsel süreci somut kararlara nasıl dönüştürdüğümüzü de şekillendirdiğini kabul eder.

Özünde, bilişsel ve karar verme tarzları arasındaki bu bağlantı, doğuştan gelen bilişsel eğilimlerimizin, kararlara karşılaştığımızda kullandığımız stratejileri önemli ölçüde etkilediğini ve bireysel karar verme farklılıklarının zengin dokusuna katkıda bulunduğunu vurgulamaktadır.

Çeşitli davranış ve tutumların, karar verme tarzları ile bağlantılı olduğu geçmiş çalışmalarda ortaya konmuştur. Bunlardan bazıları şunlardır; tüketim davranışı (Mitchell ve Walsh, 2004), kişinin kariyeri ve sağlığıyla ilgili kararlar (Galotti, 2007), kültürel kökenler (Radfordet vd., 1991) ve yeni teknolojinin değerlendirilmesi (Selart vd., 2008).

Karar verme tarzları literatürde geniş bir şekilde tanımlanır ve genellikle iki kategoriye ayrılır (Scott ve Bruce, 1995; Mau, 2000): insanların karar verirken kullandıkları

alışılmış kalıplar (Driver, 1979) ve insanların çeşitli karar verme görevlerini farklı görüntüleme ve tepki verme biçimleri (Harren, 1979).

Bu içgörülere dayanarak, Scott ve Bruce (1995) karar verme tarzlarına ilişkin önceki araştırmalardan elde edilen kolektif bilgiyi pekiştirmişlerdir (Thunholm, 2004). Karar verme tarzının şu şekilde kapsamlı bir tanımını yapmışlardır (Scott ve Bruce, 1995): "Bir karar durumuyla karşı karşıya kalan bir bireyin, sergilediği öğrenilmiş alışılmış tepki modelidir. Bu bir kişilik özelliği değil, belirli bir karar bağlamında belirli bir şekilde tepki verme eğilimine dayalı olan bir alışkanlıktır".

Bunun yaklaşımın tersine, Rowe ve Mason (1987) karar verme tarzını, bireyin problem çözmeye nasıl yaklaştığını yansıtan ve kişiden kişiye önemli ölçüde değişebilen psikolojik bir süreç olarak tanımlayarak alternatif bir bakış açısı ortaya koymuştur. Bu kapsamda, bilişsel karmaşıklığın boyutlarından yararlanarak karar verme tarzlarını tanımlayan kapsamlı bir model ortaya koymuşlardır. Önerdikleri model, bireyin karar vermede önemli bir faktör olan belirsizliğe karşı toleransını dikkate almakta; insan odaklı ve görev odaklı çalışma ortamları arasında ayırım yaparak çevresel karmaşıklığı da bünyesinde barındırmaktadır. Ortaya koydukları bu ikili vurgu, modellerinden türetilen dört farklı karar verme tarzının temelini oluşturur.

Rowe ve Mason'un (1987) çalışmalarında tanımlanan ilk karar verme tarzı, pratik ve güç odaklı bir yaklaşımla karakterize edilen "yönlendirici" tarzdır. Bu karar verme tarzına sahip bireyler, genellikle pragmatik düşüncelerle yönlendirilen basit ve kararlı eylemleri tercih ederler. Buna karşılık analitik tarz, karar vermede yapılandırılmış ve sistematik bir yaklaşımı vurgulayarak mantıksal ve göreve yönelik eğilimleri yansıtır. Kavramsal tarz, karar vermede yaratıcı, anlayışlı ve sezgisel bir yaklaşım olarak ortaya çıkar. Bu tarza sahip bireyler, yenilikçi düşünceye ve daha geniş kalıpları ayırt etme yeteneğine yönelik bir tutum sergilerler. Dördüncü tarz olan davranışsal tarz ise, karar almada insan odaklı, destekleyici ve anlayışlı bir yaklaşımın altını çizer. Bu tarza sahip bireyler, karar verme süreçlerinde kişilerarası dinamikleri ve iş birliğini ön planda tutarlar.

Rowe ve Mason (1987), özellikle dinamik ve sıklıkla değişen ortamlarda faaliyet gösteren yöneticiler için kariyer başarısına ulaşmada bilişsel tarzın kritik rolünün altını çizmektedirler. Yöneticilerin, hedeflere etkili bir şekilde odaklanmak ve gelişen çalışma ortamlarının doğasında var olan zorluklara uyum sağlamak için karar verme

tarzlarının farkında olmaları gerektiğini öne sürmektedirler. Kişinin karar verme tarzını stratejik bir varlık olarak anlamaya yönelik bu vurgu, kariyer yörüngelerinde bilişsel yaklaşımların öneminin daha geniş çapta kabul edilmesiyle uyumludur.

Bir kişinin sorunları çözmeye nasıl yaklaştığını yansıtan ve bir kişiden diğerine önemli ölçüde farklılık gösterebilen zihinsel bir prosedürün varlığı (Rowe ve Mason, 1987), bireylerin bilgiyi algılamak ve analiz etmek için farklı yöntemler kullandıklarını ve bunun da farklı karar sonuçlarına yol açtığını gösterir. Ayrıca Rowe ve Boulgarides (1992) bir kişinin karar verme tarzı hakkında bilgi sahibi olmanın karar davranışlarını tahmin etmeyi kolaylaştırabileceğini ileri sürmektedir.

Bir bireyin karar verme davranışını tahmin etme yeteneği, yalnızca siber güvenlik davranışını anlamak için değil, aynı zamanda diğer çeşitli uygulama alanları için de derin anlamlara sahiptir. Kuruluşlar, karar verme tarzlarının inceliklerini derinlemesine inceleyerek, çalışanlarının siber güvenlik uyum davranışı alanının ötesine geçen eğilimleri hakkında değerli bilgiler edinebilir. Bu öngörücü anlayış, çeşitli bağlamlarda çalışan eylemlerini ve katılımını tahmin etmeye çalışan kuruluşlar için güçlü bir araç haline gelir (Leykin ve DeRubeis, 2010).

Siber dayanıklılığın artırılması bakımından, bu öngörücü yetenek, kuruluşların uyum davranışını teşvik etmek ve uygulamak için stratejilerini uyarlamalarına olanak tanır. Karar verme tarzlarının, siber güvenlik önlemlerine yönelik bireysel tepkileri şekillendirmede önemli bir rol oynadığını kabul eden kuruluşlar, hedefe yönelik müdahaleler ve eğitim girişimlerini hayata geçirebilir (Donalds ve Osei-Bryson, 2020). Örneğin bir çalışan, mantıksal ve sistematik yaklaşımları tercih ederek karar vermede belirli bir stil sergiliyorsa, organizasyon bu bilişsel eğilimlere uygun eğitim programları uygulayabilir.

Ayrıca çalışanların karar verme tarzlarının farklılığının sonuçları hakkındaki farkındalık, kişiye özel politika ve uygulamaların geliştirilmesinde temel bir unsur oluşturmaktadır. Kuruluşlar, iş gücü içindeki farklı karar alma tarzlarına uygun siber güvenlik yönergeleri hazırlayarak daha incelikli ve etkili bir yaklaşım oluşturabilirler (Gratian vd., 2018). Bu özel strateji, çalışanların bilişsel eğilimleriyle uyumlu bir siber güvenlik kültürünü teşvik ederek başarılı uygulama ve uyumluluk olasılığını artıracaktır.

Esasen, karar verme tarzlarının proaktif olarak anlaşılması, kuruluşlara siber güvenlik veya diğer alanlardaki girişimlerini optimize etme konusunda stratejik bir avantaj sağlar. Bu bilgi, kuruluşlara insan davranışının karmaşıklıklarını yönetme gücü verir ve iş gücünde mevcut olan çeşitli bilişsel tercihlerle örtüşen hedefli müdahalelerin oluşturulmasını kolaylaştırır.

Anımsanırsa, Scott ve Bruce (1995) karar verme tarzlarını, bir kişinin bir karar verme senaryosuyla karşı karşıya kaldığında edindiği ve alışlagelmiş tepki verme şekli ve benzersiz bir sonuç için belirli bir şekilde yanıt verme alışkanlığı veya rutin odaklı bir eğilim olarak tanımlamışlardır. Karar verme tarzı araştırmasının teorik temelinde, karar verme tarzı araştırma alanında farklı araştırmaların sonuçlarını entegre edebilecek netlik eksikliği ve faydalı araçların eksikliği de gözlemlenmiştir (Scott ve Bruce, 1995). Karar vermede belirli tarzları belirlemek, beklenen davranışların sınıflandırılmasına yardımcı olabilir.

Karar tarzlarını değerlendirmeyi amaçlayan çeşitli araştırmalar yürütülmüş (Mann, 1982; Scott ve Bruce, 1995; Nygren, 2000) ve her biri karar vermede belirli bir tarz aralığını hedef almıştır. Bu sorgulama biçimleri sıklıkla bazı alt bölümlerde önemli ölçüde örtüşme sergilemektedir. Örnek olarak, Nygren'in (2000) aracındaki analitik alt bölüm, Scott ve Bruce'un (1985) anketindeki rasyonel alt bölüme benzerlik göstermekte ve Mann'ın (1982) anketindeki ihtiyat alt bölümüne benzemektedir. Benzer şekilde, Mann'ın (1982) anketindeki savunmadan kaçınma alt ölçeği, Scott ve Bruce'un (1985) anketindeki hem kaçınan hem de bağımlı alt ölçeklerle aynı özellikleri paylaşmaktadır. Bu araçların her birinin kendine özgü alt ölçekleri de bulunmaktadır.

Bu tezde katılımcıların karar verme tarzlarını değerlendirmek amacıyla Scott ve Bruce (1995) tarafından oluşturulan Genel Karar Verme Tarzı Envanteri (GKVT) kullanılmıştır. Bu araç, karar tarzlarına ilişkin geniş bir bakış açısı sunmakta ve karar verme tarzlarını değerlendirmede en bilinen ve en kapsamlı şekilde araştırılan ölçeklerden biri olarak öne çıkmaktadır (Allwood ve Salo, 2012). Karar vermede tarzlara göre ayırt edici özellikler ve eğilimler ortaya çıkmaktadır.

Scott ve Bruce (1995) davranışsal özelliklere dayalı olarak karar vermede dört tarz belirlemiş ve özetlemiştir. Rasyonel tarz, verilerin kapsamlı bir şekilde aranmasını, alternatiflerin envanterini ve makul değerlendirmeyi içerir. Sezgisel tarz, bilgi akışındaki ayrıntılara odaklanır ve sistematik işleme yerine önsezileri ve duyguları

tercih eder. Bağımlı tarz, seçenekleri seçmeden önce tavsiye ve talimat isterken, kaçınma tarzı her fırsatta karar almaktan kaçınır. Genel Karar Verme Tarzı Envanteri (GKVT) çalışmasının, bir subay örnekleme ile doğrulanan ilk formu, beşinci bir tarz olan spontane tarzı ortaya çıkarmıştır. Spontane tarz, hızlı karar alma arzusuyla belirginleşmektedir. Öğrenci, mühendis ve teknisyen örnekleriyle yapılan müteakip doğrulamalar, çeşitli karar bağlamlarında sürekli olarak beş faktörlü bir modeli doğrulamıştır. Korelasyon analizleri, kendiliğinden ve sezgisel tarzlardaki pozitif korelasyonlar ve rasyonel ve diğer tarzlardaki negatif korelasyonlar gibi belirli tarzlar arasındaki ilişkileri göstermiştir.

Doğrulama çalışmaları karar verme tarzlarına ilişkin bilgiler sağlamıştır. Örneğin, rasyonel karar verme tarzı, erkek teknisyenler ve mühendisler arasında yaratıcı eylemlerin bütünleşik bir göstergesinin yanı sıra, iç kontrol merkezi ile pozitif korelasyonlar ve yaratıcılık ile negatif korelasyonlar göstermiştir (Scott ve Bruce, 1995). Russ vd. (1996), rasyonel karar verme tarzı ile birinci düzey pazarlama yöneticilerinin liderlik kapasitesinin çok boyutlu bir değerlendirmesi arasında pozitif bir ilişki olduğunu ortaya çıkarmıştır. Ancak karar verme tarzları ile liderlik stilleri (işlemsel ve dönüşümsel) arasında herhangi bir ilişki bulamamışlardır.

Scott ve Bruce'a (1995) göre, karar vermedeki sezgisel tarz, kontrol odağıyla bir korelasyon göstermemekte, kontrol yöneliminden bağımsız olarak yaygın olduğunu göstermektedir. Ancak üstlerin yaratıcılık puanları ile pozitif fakat çok anlamlı olmayan bir korelasyona sahip olduğu bulunmuştur. Simüle edilmiş bir ortamda yürütülen ve iletişim yapılarının performansın verimliliği üzerindeki etkisini değerlendiren bir çalışmada Omodei vd. (2000), bir liderin sezgisel karar verme tarzının, sınırlandırılmış kişilerarası bir ortamda verimliliği engellediğini, ancak serbest akışlı bir etkileşim yapısında olağanüstü sonuçlara olanak sağladığını gözlemlemiştir.

Scott ve Bruce (1995) tarafından ana hatlarıyla belirtildiği gibi, karar vermedeki bağımlı tarz, kontrol için dış bir noktada bir korelasyon sergiler; bu durum ise, bağımlı tarza sahip bireylerin, kaderleri üzerinde otoriteyi, kavrayışlarının ötesindeki değişkenlere atfettiklerini göstermektedir. Ayrıca, teknisyen ve mühendislerden oluşan erkek bir örneklem grubu için, üstlerin yaratıcılık değerlendirmeleri ve yaratıcı düşüncenin genel göstergesi ile negatif bir korelasyona sahip olduğu bulunmuştur.

Scott ve Bruce (1995), karar vermedeki kaçınma tarzının, dışarıdan kontrol etme yönelimiyle ilişkili olduğunu tespit etmiştir. Başlangıç seviyesindeki pazarlama yöneticilerinin yönetsel etkililik dereceleri ile karar vermede kaçınma tarzı arasında negatif bir ilişki gözlemlenmektedir (Russ vd., 1996). Ek olarak, karar vermede kaçınma tarzı ile çatışma yönetimi arasında pozitif bir ilişki keşfedilmiştir; bu ise, karar vermede kaçınma tarzı bireylerin aynı zamanda çatışmalarla kaçınmacı bir şekilde başa çıkma eğiliminde olduklarını göstermektedir (Loo, 2000).

Ancak bu tez örneğinde, spontane ve kaçınma tarzlarından yetersiz katılımcı gözlemlenmiştir. Ancak diğer karar verme tarzları (bağımlı, sezgisel, rasyonel) Harren'in (1979) karar verme tarzları taksonomisi ile örtüşmektedir. Harren'in (1979) rasyonel, sezgisel ve bağımlı tarzlar arasındaki ayrımı, karar verme tarzlarına ilişkin birçok taksonomik sınıflandırma arasında en sık kabul edilen, kavramsal olarak sağlam ve en sade olanıdır (Singh ve Greenhaus, 2004; Mau, 2000; Phillips vd., 1985).

Aşağıdaki bölüm, Koruma Motivasyonu Teorisi (KMT) kapsamında siber güvenlik uyum davranışını ve dinamiklerini açıklamaktadır.

2.2. Siber Güvenlik Uyum Davranışı ve Koruma Motivasyonu Teorisi

Araştırmanın bağımlı değişkeni olan siber güvenliğe uyum davranışları, her bireyin karar verme tarzı belirlendikten sonra teorik olarak açıklanmıştır. Literatürde insanların güvenliğe uyum davranışlarını açıklamak için geniş bir fikir yelpazesi kullanılmıştır. Mevcut tezde insanların siber güvenlik uyum davranışlarını analiz etmek için genellikle bilgi güvenliği literatüründe adı geçen Koruma Motivasyonu Teorisi (KMT) (Burns vd., 2017) kullanılacaktır.

Rogers (1983) tarafından geliştirilen Koruma Motivasyonu Teorisi, esasen sosyal psikoloji ve sağlık alanlarında, sağlıkla ilgili inanç modelinin genişletilmiş hâlidir (Rippetoe ve Rogers, 1987). Rogers'a (1975, 1983) göre Koruma Motivasyonu Teorisi, insanların tehlikeler veya zararlı davranışlarla ilgili uyarılara nasıl tepki vermeye yönlendirildiğini açıklamaktadır. Farklı bir ifadeyle teorinin temel ilkesi, insanların algılanan tehlike karşısında kendilerini savunmaya yöneldikleri düşüncesidir (Youn, 2005).

Rogers tarafından (1975) kavramsallaştırılan Koruma Motivasyonu Teorisi, başlangıçta korku çekiciliğinin etkisini açıklamayı amaçlayan teorik bir perspektif olarak tasarlanmıştır. Rogers'ın (1983) Koruma Motivasyonu Teorisinde daha sonra yaptığı değişiklik, davranış değişimlerini kolaylaştıran bilişsel mekanizmalara odaklanarak ikna edici etkileşimlerin etkilerine ilişkin daha kapsamlı bir açıklama sunarak kapsamını genişletmiştir. Gelişimini takiben, araştırma çabaları ağırlıklı olarak iki yaklaşımı benimsemiştir: birincisi, Koruma Motivasyonu Teorisini ikna edici etkileşimleri oluşturmak ve değerlendirmek için bir yapı olarak kullanmak ve ikinci ise, Koruma Motivasyonu Teorisini sağlıkla ilgili eylemleri tahmin etmek için öngörücü bir model olarak kullanmaktır.

Koruma Motivasyonu Teorisinin kökleri, özellikle korkuya başvurma davranış ve tutumları etkileyebileceği koşulların araştırılmasında, korku çekiciliğinin ikna edici etkisi üzerine yapılan ilk araştırmalara kadar uzanmaktadır. Hovland vd.'nin (1953) temel çalışması, korku çekiciliğinin davranış ve tutumlarda nasıl değişikliklere yol açabileceğini sistematik olarak araştırmıştır. Çalışma, korkunun deney eylemlerini teşvik eden etkili bir faktör olduğunu ileri sürerek korkuya dayalı davranış modeline dayanmaktadır. Bu modele göre, bir iletişim korkuya neden olduğunda, alıcı bu nahoş ruh hâlini hafifletmeye teşvik edilir. Etkileşim davranışsal rehberlik içerdiğinde ve bunu takiben tehlike izlenimi azaldığında, davranışsal tepki güçlenerek daha sonraki başarı olasılığını artırır. Tersine, eğer davranışsal tavsiyelere uymak korkuyu azaltamazsa veya iletişimde böyle bir rehberlik yoksa, bireyler korkuyu azaltmak için kaçınma veya inkâr gibi alternatif uyumsuz başa çıkma stratejilerine başvurabilirler (Norman vd., 2015).

Korkuya dayalı davranış modeli, korkunun uyarılması ile önerilen rehberliği alma olasılığı arasında düzensiz bir korelasyon olduğunu öne sürerek monoton olmayan bir ilişki olduğunu öne sürmüştür. Janis (1967), bireyleri tehlikeyi azaltmanın (kolaylaştırma) yollarını aramaya motive etmenin ötesinde, korkunun önerilen rehber hakkında daha kapsamlı bir değerlendirmeyi de teşvik edebileceğini ileri sürmüştür. Bu perspektife göre korku sıfırdan yükseldikçe yardımların müdahaleden daha hızlı artması beklenmektedir. Ancak arzu edilen bir sınırın ötesinde, korkunun yıkıcı sonuçlarının, cesaret verici sonuçlarından daha hızlı büyüdüğüne inanılmaktadır. Sonuç olarak teori, korkunun uyarılması ile aktivite rızası arasında ters U şeklinde bir bağlantı olduğunu öngörmektedir. Bu kavramsal iddialardan bağımsız olarak, bu ters

U şeklindeki bağlantıyı destekleyecek çok az kanıt vardır (Leventhal, 1970). Aksine, Sutton (1982), 1953 ve 1980 yılları arasında yürütülen ilk araştırmaların incelemesinde, pozitif olan doğrusal bir ilişkinin daha güçlü bir şekilde doğrulandığını keşfetmiştir.

Rogers (1975), korkuya hitap eden önemli faktörleri ve bunların psikolojik aracılık sonuçlarını belirlemek amacıyla, korku çekiciliğinin teorik anlayışını geliştirmek için Koruma Motivasyonu Teorisini geliştirmiştir. Hovland vd.'ne (1953) göre Koruma Motivasyonu Teorisi, korku çekiciliğinde şu üç temel uyaran değişkenini birleştirir: (1) bir olayın ciddiyeti, (2) olayın koruyucu davranış benimsenmeden meydana gelme olasılığı ve (3) önerilen başa çıkma tepkisinin etkinliği. Rogers (1975), her tetikleyici faktörün ilişkili bir psikolojik aracılık yöntemini harekete geçirdiğini iddia ederek bu faktörleri ilk Koruma Motivasyonu Teorisi (KMT) bileşimine yerleştirmiştir. Sonuç olarak, bir olayın ciddiyeti, ciddiyet algısını tetikler, olayın gerçekleşme olasılığı kırılganlığa dair inançları tetikler ve başarılı bir başa çıkma tepkisinin erişilebilirliği, tepki verimliliğine ilişkin görüşleri tetikler. Temelde, algılanan önem derecesi, kırılganlık ve yanıt etkinliği, korku çekiciliğinde uyarıcı değişkenlerin etkisini hafifletir. Buna karşılık, bu algılar, davranışsal rehberliği takip etme arzusunu temsil eden koruma motivasyonunu şekillendirir. Koruma motivasyonu, koruyucu davranışın yakın belirleyicisi olarak kabul edilir ve "aktiviteyi uyandırmaya, sürdürmeye ve yönlendirmeye" hizmet eder (Rogers, 1975).

Rogers (1983) Koruma Motivasyonu Teorisinde revizyonlar yaparak kapsamını ikna edici iletişime ve buna aracılık eden psikolojik mekanizmalara ilişkin daha geniş bir kavramı kapsayacak şekilde genişletmiştir. Güncellenmiş versiyon, ikna edici iletişimlerin ötesinde, örneğin gözlem yoluyla öğrenme, önceki deneyimler ve kişilik özellikleri gibi bilişsel süreçleri başlatan faktörleri kapsamaktadır. Tehdidin değerlendirilmesi ve başa çıkmanın değerlendirilmesi olarak sınıflandırılan ek psikolojik aracılı prosedürleri kapsayacak şekilde büyümüş ve uygunsuz yanıtların faydaları, öz yeterlik ve yanıt maliyetleri gibi faktörleri içermektedir.

Koruma Motivasyonu Teorisini oluşturan iki farklı değerlendirme prosedürü, tehdit değerlendirmesi ve başa çıkma değerlendirmesidir. Bu temel prosedürler, insanların kendilerini tehlikeli durumlara sokmaya nasıl teşvik edildiğini öğrenmeyi amaçlamaktadır. Tehdit değerlendirmesi, insanların tehlikeleri nasıl gördüğünü

açıklamak için algılanan güvenlik açığı ve ciddiyet gibi faktörleri dikkate alır. Tepki yeterliliğini, algılanan engelleri ve öz yeterliği kapsayan baş etme değerlendirmesi, insanların başa çıkma ve bir tehlikeden kaynaklanan potansiyel hasarı veya zararı önleme kapasitesini nasıl değerlendirdiğini açıklar (Woon vd., 2005; Ifinedo, 2012).

Daha ayrıntılı bir şekilde ifade etmek gerekirse, Koruma Motivasyonu Teorisindeki tehdit değerlendirmesi, inkâr ve kaçınma gibi uyumsuz tepkilerin olasılığını etkileyen faktörlere odaklanır. Uyumsuz tepkiler, ciddiyet ve kırılganlık hakkındaki inançlar tarafından engellenir ve korku, araya giren bir değişken olarak hareket eder. Ciddi bir tehdide karşı algılanan hassasiyetin artması, koruyucu davranışa yönelik korkuyu ve motivasyonu artırır. Bu engelleyici faktörlere rağmen, dışsal (örneğin, sosyal onay) ödüller ve içsel (örneğin, zevk), sigara içenlerin sigara içmenin kilo vermelerine veya sosyalleşmelerine yardımcı olduğunu varsaymaları gibi, uyumsuz tepkilerin olasılığını artırabilir. Koruma Motivasyonu Teorisinde başa çıkmanın değerlendirilmesi, mevcut başa çıkma yanıtlarını ve davranışsal tavsiyeleri takip etmek gibi uyarlanabilir yanıtları etkileyen faktörleri ele alır. Önerilen davranışın etkililiğine (tepkinin etkililiği) ve kişinin bunu gerçekleştirme kapasitesine (öz yeterlik) inanmak, uyarlanabilir bir tepki olasılığını artırır. Örneğin, sigara içenler sigarayı bırakmanın akciğer kanseri riskini nasıl azalttığını ve sigarayı bırakıp bırakamayacaklarını değerlendirebilirler. Bu arttırıcı faktörlere rağmen, sigara içenler sigarayı bıraktıktan sonra artan istekten korkabilecekleri için engeller veya müdahale maliyetleri (örneğin kaynak bulunabilirliği) uyum sağlama davranışını engelleyebilir (Norman vd., 2015).

Literatürde Koruma Motivasyonu Teorisi, insanların tehdit veya tehlikeli davranışlarla karşı karşıya kaldıklarında neden koruyucu eylemlerde bulunduğunu açıklamaya odaklanan yapısı nedeniyle siber güvenlik uyumu bağlamını (davranış veya niyet) açıklamak için başarıyla uygulanmıştır (Li vd., 2019; Safa vd., 2015; Vance vd., 2012; Siponen ve Vance, 2014; Crossler ve Belanger, 2014; Ifinedo, 2012).

Koruma Motivasyonu Teorisinin hem davranışı hem de niyeti kapsayan siber güvenlik uyumu bağlamını açıklamada değerli bir yapı olduğu kanıtlanmıştır. Bu benimseme, bireylerin potansiyel tehditler veya tehlikeli davranışlar karşısında neden koruyucu eylemleri tercih ettiklerinin inceliklerini çözmeye odaklanan Koruma Motivasyonu Teorisinin doğal yapısından kaynaklanmaktadır. Koruma Motivasyonu Teorisi, siber güvenlikle ilgili karar vermenin altında yatan bilişsel süreçleri derinlemesine

inceleyerek bireyleri güvenlik önlemlerine uymaya yönlendiren motivasyon faktörlerinin kapsamlı bir şekilde anlaşılmasını sağlar (Li vd., 2019). Başlangıçta korku çağrılarına verilen tepkileri açıklamak için geliştirilen bu teorik çerçeve, çok yönlülüğü ve koruyucu davranışları etkileyen psikolojik yönler üzerine vurgu yapması nedeniyle siber güvenlik alanında uygulanabilmektedir. Araştırmacılar ve akademisyenler, siber güvenlik uygulamalarına ilişkin tepki ve öz yeterlik, algılanan tehdit ve güvenlik açığı arasındaki incelikli etkileşimi keşfetmek için Koruma Motivasyonu Teorisinden yararlanmıştır. Koruma Motivasyonu Teorisinin siber güvenliğin dinamik ortamına uyarlanabilirliği, dijital güvenlik alanında insan davranışının karmaşıklığını çözmedeki faydasını vurgulamaktadır.

Bir sonraki bölümde, yukarıda sunulan teorik temellerin ışığında, çalışmada önerilen kavramsal modelin detayları açıklanmaktadır.

2.3. Kavramsal Model

Tez kapsamında çalışmanın bağımlı değişkeni olan siber güvenlik uyum davranışlarını incelemek amacıyla kavramsal bir model oluşturulmuştur.

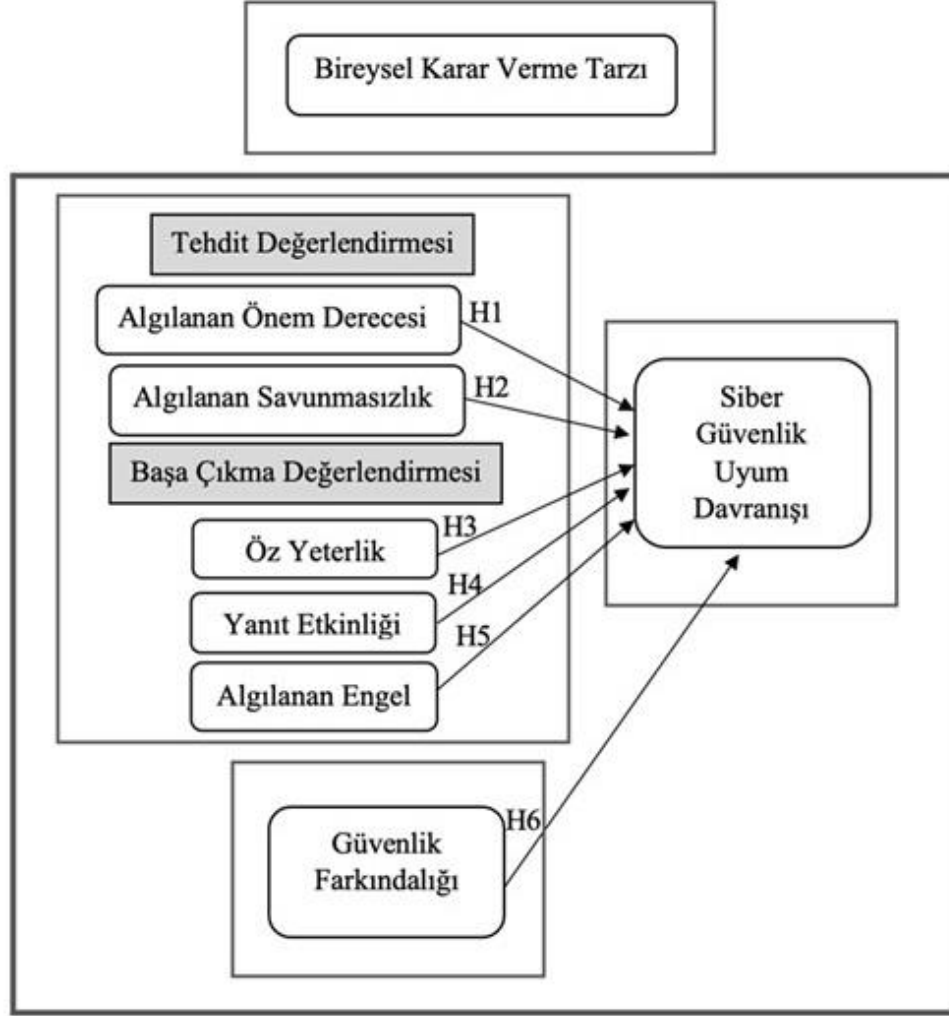
Koruma Motivasyonu Teorisi çerçevesinde, Koruma Motivasyonu Teorisinin iki temel değerlendirme süreci olan tehdit değerlendirmesi ve başa çıkma değerlendirmesi, bağımlı değişkeni incelemek için modele dâhil edilmiştir. Tehdidin değerlendirilmesi; algılanan savunmasızlık ve algılanan önem derecesi faktörlerini içerir ve bireylerin siber tehditleri nasıl algıladıklarını açıklamak için modele dâhil eklenmiştir. Başa çıkmanın değerlendirilmesi; yanıt etkinliğini, öz yeterliliği ve algılanan engel faktörlerini içerir ve bu faktörler, bireylerin bir siber saldırıdan kaynaklanan potansiyel hasarı veya zararı yönetme ve engelleme yeteneklerini değerlendirme şeklini açıklamak için modele eklenmiştir.

Güvenlik farkındalığı, siber güvenliğe uyum davranışını açıklayan literatürde sık kullanılan bir faktördür. Tez kapsamında güvenlik farkındalığı faktörünün kavramsal modele dâhil edilmesiyle siber güvenlik farkındalığının siber güvenliğe uyum üzerindeki etkisinin, bu etkinin karar verme tarzlarına göre farklılaşp farklılaşmadığının, farklılaştıysa nasıl farklılaştığının araştırılması amaçlanmaktadır.

Araştırmanın parametreleri kapsamında, kavramsal modelde yer alan bağımsız değişkenlerin bağımlı değişken üzerindeki etkileri genel olarak incelenmenin yanı sıra,

bu etkilerin bireylerin karar verme tarzlarına göre farklılık gösterip göstermediği, gösteriyorsa bunun ne ölçüde etkili olduğu sonucuna da varılmaya çalışılmıştır.

Geliştirilen kavramsal model **Şekil 2.1**'de sunulmuştur;



Şekil 2.1: Kavramsal Model.

Geçmişte yapılan çalışmaların ışığında, her bir bağımsız değişken ile bağımlı değişken arasındaki ilişkileri araştırmak için hipotezler geliştirilmiştir. Bu hipotezler yukarıdaki modelde numaralandırılarak gösterilmiştir. Hipotez geliştirme tartışmaları aşağıda sunulmuştur.

2.4. Hipotez Geliştirme

Önceki tartışmaların ışığında, hipotezlerin formülasyonu, çeşitli bağımsız değişkenler ile bağımlı değişken arasındaki ilişkileri sistematik olarak araştırmak ve test etmek için

hayati önem taşımaktadır. Bu bölümde geçmiş çalışmalardan elde edilen bilgilere dayanarak geliştirilen hipotezler özetlenmektedir. Yukarıdaki modelde karşılık gelen numaralandırmayla gösterilen her hipotez, tanımlanan değişkenler arasındaki karmaşık dinamiklere ilişkin anlayışımızı geliştirmeyi amaçlayan test edilebilir bir öneri olarak hizmet etmektedir. Bu hipotezler, ampirik araştırmaların önünü açmakta ve siber güvenlik uyum davranışını etkileyen faktörlere ilişkin devam eden söylemlere katkıda bulunmaktadır.

2.4.1. Siber Güvenlik Uyum Davranışı ve Algılanan Önem Derecesi

Koruma Motivasyonu Teorisinin temel önermesi, bireylerin tehlikeli durumlardan algılanan tehditlere yanıt olarak motive olmaya ve kendilerini korumaya yönlendirildikleridir (Youn, 2005). Sonuç olarak, Koruma Motivasyonu Teorisi çerçevesinin, bireylerin bir risk faktörü olarak siber güvenlik riskleriyle karşı karşıya kaldıklarında kurumlarının veri kaynaklarını korumak için benimseyebilecekleri davranışlara dair içgörü sağlayabileceği sonucuna varılmıştır. Koruma Motivasyonu Teorisinin tehdit faktörlerine ilişkin değerlendirmesinin bir bileşeni olan algılanan önem derecesi, bir kişinin potansiyel bir güvenlik riskinin ciddi bir zarar verme ve önemli rahatsızlıklara yol açma potansiyeline sahip olduğu yönündeki değerlendirmesini gerektirir (Herath ve Rao, 2009a).

Siber güvenlik alanında tehdit, kurumsal bir bilgi sisteminin yetkisiz bir şekilde ele geçirilmesi olarak ortaya çıkabilir ve bu da kritik bilgi varlıklarının açığa çıkmasına yol açabilir. Bu bağlamda algılanan önem derecesi, açıklanan bilgilerin kuruluş üzerinde yaratabileceği potansiyel etkinin değerlendirilmesini içerir. Bulgurcu vd. (2010) ve Pahnla vd. (2007) tarafından yapılan çalışmalarda da belirtildiği gibi, kurumlarının bilgi teknolojileri kaynaklarının saldırı altında olduğuna inanan kişiler uyum eylemleri gerçekleştirme eğilimindedir.

Vance vd. (2012), algılanan önem derecesinin örgütsel bir ortamda çalışanların güvenlik niyetlerini etkilemede önemli bir rol oynadığını doğrulamıştır. Benzer şekilde, diğer araştırmalar algılanan önem derecesi ile çevrimiçi tüketim (Larose vd., 2005), antivirüs kullanımı (Lee vd., 2008) ve sosyal medya platformlarıyla etkileşim (Mohamed ve Ahmad, 2012) dâhil olmak üzere çeşitli bağlamlarda siber güvenlik uyum davranışı arasında pozitif bir ilişki tespit etmiştir.

Sonuç olarak, uyum davranışı sergilememenin ciddi sonuçlar doğuracağını düşünen çalışanların siber güvenlik düzenlemelerine uyum sağlama eğiliminde oldukları varsayılmaktadır. Buradan hareketle;

H1: Çalışanların algılanan önem derecesi, siber güvenlik önlemlerine uyma davranışlarını olumlu yönde etkilemektedir.

2.4.2. Siber Güvenlik Uyum Davranışı ve Algılanan Önem Derecesi Algılanan Savunmasızlık

Koruma Motivasyonu Teorisinde tehdit değerlendirmesinin ikinci faktörü olan algılanan savunmasızlıktır. Siber güvenlik açısından algılanan savunmasızlık, insanların bir siber saldırının oluşturduğu yakın tehlikeyi ne ölçüde algıladıkları ve bu tehlikeyi hafifletmeye yönelik teknik ve araçlarla yetersiz donanımına sahip olduklarını algılama derecesini kapsamaktadır (Vance vd., 2012). Kurumun bilgi sisteminde yüksek düzeyde savunmasız hisseden çalışan, koruyucu davranışlarda bulunmaya daha yatkındır (Ifinedo, 2012).

Bu düşünceyle tutarlı olarak Lee vd. (2008), internet virüslerine karşı yüksek düzeydeki güvenlik açığının, insanların virüsten korunma niyetini artırdığını keşfetmiştir. Sonuç olarak, virüsle ilgili tehditlere karşı algılanan savunmasızlık ne kadar yüksek olursa, bireylerin virüsten korunmayı benimseme olasılığı da o kadar artmaktadır. Özelemek gerekirse, bireyler olası virüs saldırılarına karşı artan güvenlik açığı hissine yanıt olarak, güçlü bir antivirüs yazılımı kurmak veya siber güvenlik protokollerini tekrar tekrar güncellemek gibi proaktif önlemler almaya motive olmaktadır.

Çeşitli çalışmalar, algılanan savunmasızlığın, iş liderlerinin şirketlerinde güvenlik araçlarını kullanma niyetleri (Lee ve Larsen, 2009), sosyal ağ sitelerindeki bilgi gizliliğine ilişkin endişeler (Mohamed ve Ahmad, 2012), personelin kişisel özellikleri bildirilen siber güvenlik eylemleri (Anwar vd., 2017) ve çalışanların siber güvenlik uyumları (Li vd., 2019) gibi faktörler üzerindeki etkisini göstermiştir. Algılanan savunmasızlığın bireylerin siber güvenlik davranışlarını önemli ölçüde etkilediği önermesinden yola çıkan bu çalışma, kurumun bilgi sistemine yönelik savunmasızlık algısının artmasının siber güvenlik uyum davranışı eğiliminin artmasına yol açacağını öngörmektedir. Sonuç olarak;

H2: Çalışanların algılanan savunmasızlık derecesi, siber güvenlik önlemlerine uyma davranışlarını olumlu yönde etkilemektedir.

2.4.3. Siber Güvenlik Uyum Davranışı ve Algılanan Öz Yeterlik

Koruma Motivasyonu Teorisinin tehdit değerlendirme faktörlerine (algılanan önem derecesi ve algılanan savunmasızlık) ek olarak, başa çıkma değerlendirmesi faktörleri (öz yeterlik, yanıt etkinliği ve algılanan engel) ile siber güvenlik uyum davranışı arasındaki ilişkiler hakkında hipotezler de ortaya koyulmuştur.

Koruma Motivasyonu Teorisinde başa çıkma değerlendirmesinin ilk faktörü olan öz yeterlik, insanların potansiyel siber saldırılarla ilişkili tehlikeleri azaltmak için önleme eylemlerini uygulama konusundaki yeteneklerine, uzmanlıklarına veya kapasitelerine ilişkin değerlendirmesiyle ilgilidir (Vance vd., 2012; Bulgurcu vd., 2010).

Kendilerini siber güvenliğe yönelik koruyucu davranışlarda bulunma kapasitesine sahip olarak algılayan çalışanların, kuruluşları tarafından önerilen yönergelerle uyma olasılıklarının daha yüksek olduğunu varsaymak mantıklıdır. Dahası, çalışanların koruyucu davranışları benimseme yeteneklerine duydukları güvenin, yalnızca kurumsal kurallara bağlılığı teşvik etmekle kalmayıp aynı zamanda işyerinde proaktif bir siber güvenlik kültürünü de geliştirdiğini varsaymak akla yatkındır. Bunun tersine, önerilen yönergelerle uyulmaması, belirli güvenlik standartlarının ne zaman kullanıldığını tespit etme konusunda algılanan yetenek, anlayış veya uzmanlık eksikliğinden kaynaklanabilir (Leering vd., 2022).

Bu görüşü destekleyen Donalds ve Osei-Bryson (2020), bireylerin öz yeterliğinin, şifre güvenliği ve genel güvenlik uyumu ile ilgili davranışlarını etkilediğini keşfetmiştir. Bu bulgular, öz yeterlik ile çeşitli bilgi güvenliği davranışları arasında pozitif bir ilişki kuran benzer çalışmalarla da uyumludur. Örneğin Ifinedo (2012), çalışanlar arasındaki öz yeterlik ile bilgi sistemleri güvenlik prosedürlerine davranışsal bağlılık arasındaki ilişkiyi vurgulayan somut kanıtlar sunmaktadır. Anwar vd. (2017) benzer şekilde öz yeterlik ile çalışanların kendilerinin bildirdiği siber güvenlik davranışları arasında pozitif bir bağlantı tespit etmiştir. Ayrıca, ek bulgular öz yeterliğin siber güvenlik uyum davranışını önemli ölçüde etkilediğine işaret etmiştir (Bulgurcu vd., 2010; Ng vd., 2009; Li vd., 2019; D'Arcy ve Lowry, 2019).

Bu nedenle, siber uzaya ilişkin risklere karşı koruyucu önlemleri hayata geçirebileceklerine inanan çalışanların, siber güvenlik önlemlerine uyum gösterme eğilimi daha yüksektir;

H3: Çalışanların öz yeterlik derecesi, siber güvenlik önlemlerine uyma davranışlarını olumlu yönde etkilemektedir.

2.4.4. Siber Güvenlik Uyum Davranışı ve Yanıt Etkinliği

Yanıt etkinliği, Koruma Motivasyonu Teorisinin başa çıkma değerlendirmesinin diğer faktörlerinden biridir. Bir tehlikeye karşı öngörülen karşı eylemin riski başarılı bir şekilde azaltacağı fikrini ifade eder (Ifinedo, 2012).

Bilgi güvenliği bağlamında bu, insanların, kurumlarının bilgi sistemlerine yönelik güvenlik prosedürlerinde belirtilen kural ve düzenlemelerin potansiyel tehditleri gerçekten azaltacağına dair güveni anlamına gelir. Mevcut politikaların belirlediği aksiyonları uyguladığında tehditleri ortadan kaldıracığına inanan ve bu talimatlara güvenen bir çalışanın, talimatlara uyma konusunda özenli olmasını beklemek makul olacaktır. Kurumlarının bilgi güvenliği prosedürleri sistemlerinin etkili olduğuna inanan çalışanlar, bunları benimsemeye ve bunlara uymaya daha yatkındır (Herath ve Rao, 2009a).

Bu anlayış, özellikle ev içi kablosuz güvenlik alanında yanıt etkinliği ve koruyucu siber güvenlik davranışı ile pozitif bir ilişki olduğunu tespit eden Woon vd.'nin (2005) sonuçlarında da ortaya çıkmaktadır. Lee ve Larsen (2009) güvenlik araçlarının organizasyonlarda benimsenmesi bağlamında da aynı pozitif ilişkiyi keşfetmişlerdir. Diğer çalışmalar, bu ilişkiyi, insanların güvenlik yönergelerini ve politikalarını takip etmeye hazır olmaları (Vance vd., 2012) ve insanların genel siber güvenlik uyum davranışları (Li vd., 2019) dâhil olmak üzere çeşitli bağlamlarda doğrulamaktadır.

Bu nedenle, kuruluşlarının siber uzayla ilgili riskleri azaltmak için önerilen müdahalesinin etkinliğine güvenen çalışanların, siber güvenlik önlemlerine uyum göstermeye daha yatkın olmalarını öneriyoruz;

H4: Çalışanların yanıt etkinliklerinin derecesi, siber güvenlik önlemlerine uyma davranışlarını olumlu yönde etkilemektedir.

2.4.5. Siber Güvenlik Uyum Davranışı ve Algılanan Engel

Algılanan engel, Koruma Motivasyonu Teorisinin başa çıkma değerlendirilmesinde başka bir bileşeni oluşturur. Bu engeller, bireylerin müdahale maliyetlerine ilişkin algılarını kapsar ve siber güvenlik koruma davranışını gerçekleştirmenin hoş olmayan veya uygunsuz yönlerini belirtir (Ng vd., 2009).

Daha basit bir ifadeyle, algılanan engeller, bireylerin siber güvenlik tehditlerine karşı korunmak için belirli eylemleri gerçekleştirmeye ilişkilendirdiği algılanan dezavantajları veya zorlukları içerir. Örneğin, çalışanlar önerilen siber güvenlik önlemlerini zaman alıcı, karmaşık veya normal iş akışlarını bozucu olarak görebilir ve bu koruyucu davranışların uygulanmasıyla ilgili rahatsızlık veya rahatsızlık hissine katkıda bulunabilir.

Çalışanlar bir kuruluşun önerilen müdahalesinin bir tehdidi ortadan kaldıracabileceğine inansa da bu onların o eylemi gerçekleştirme istekliliğini garanti etmez. Önerilen yanıtın bir tehdidi önleyebileceği bilgisine rağmen, bireyler bunu hoş olmayan veya uygunsuz olarak algılayabilir, bu da algılanan engeller olarak adlandırılan duruma yol açabilir ve potansiyel olarak siber güvenlik uyum davranışını engelleyebilir. Aslında önceki araştırmalar, bariyer algısı ile güvenlikle ilgili çeşitli eylemler arasında sürekli olarak olumsuz bir ilişki olduğunu göstermiştir (Vance vd., 2012; Herath ve Rao, 2009a; Anwar vd., 2017; Li vd., 2019).

Sonuç olarak beklentimiz, çalışanların algıladığı engellerin siber güvenlik önlemlerine uyum ile olumsuz bir ilişki sergileyeceği yönündedir. Öyleyse;

H5: Çalışanların algıladıkları engellerin derecesi, siber güvenlik önlemlerine uyma davranışlarını olumsuz yönde etkilemektedir.

2.4.6. Siber Güvenlik Uyum Davranışı ve Güvenlik Farkındalığı

Güvenlik farkındalığı, siber güvenlik uyumluluğu bağlamında temel değişkenlerden biridir. Bireylerin gelişen siber tehditlere karşı proaktif bir savunma inşa etmelerinin temelini oluşturmaktadır. Siber güvenliğin dinamik ortamında, birey arasında güçlü bir güvenlik farkındalığı oluşturmak, bilinçli karar alma ve siber güvenliğin iyi uygulamalarına proaktif bağlılık için güçlü bir katalizör görevi gördüğünden çok önemli bir etkidir.

Güvenlik farkındalığı, insanların güvenlik sorunlarını ve bunların siber olayların olası sonuçlarını genel olarak kavramasıyla ilgilidir (Bulgurcu vd., 2010). Güvenlik farkındalığının önemi, bireyleri siber tehditlerin ciddiyetini anlama, bilinçli seçimler yapma ve dirençli bir siber güvenlik kültürüne aktif olarak katkıda bulunma konusunda güçlendiren yol gösterici bir güç rolünde açıkça ortaya çıkmaktadır. Dolayısıyla güvenlik farkındalığı, insanları siber hijyen ilkelerine bağlayan, bilinçli ve proaktif eylemler yoluyla siber tehditleri engelleme konusunda kolektif bir kararlılığı teşvik eden bir bağlıdır.

Kuruluşları siber saldırılara karşı korumak için sağlam bir teknolojik altyapı gerekli olsa da çalışanların farkındalığının artırılması da aynı derecede önemlidir (Li vd., 2019). Teknolojinin sınırlarının ötesinde güvenlik farkındalığı, davranışsal siber güvenlik ortamında kritik bir faktör olarak ortaya çıkmakta ve potansiyel riskler ve önleyici tedbirler konusunda keskin bir anlayış yoluyla bireyleri dijital varlıkların dikkatli koruyucularına dönüştürmektedir.

Potansiyel siber tehditlerin ve bunların sonuçlarının bilincinde olan bir çalışanın, kurumu tarafından önerilen güvenlik önlemlerine uyma olasılığının daha yüksek olacağını varsaymak mantıklı olacaktır. Bu varsayımın ardındaki mantık, potansiyel siber tehditler ve bunların etkileri konusunda farkındalığa sahip bir çalışanın, doğası gereği, kuruluşları tarafından öngörülen güvenlik önlemlerini benimsemeye ve bunlara uymaya daha yatkın olduğunun ve dijital risklere karşı koruma konusunda proaktif bir kararlılık gösterdiğinin anlaşılmasında yatmaktadır.

Güvenlik farkındalığı ile siber güvenlik davranışı arasındaki ilişki, farklı bağlamlarda yapılan çok sayıda araştırmayla kurulmuştur. Örneğin, çalışmalar bir kişinin şifre değiştirme zamanı ile güçlü şifre kullanma eğilimi arasındaki ilişkiyi (Stanton vd., 2005), kullanıcıların Bilgi Güvenliği Politikası uyumluluğuna ilişkin niyetlerin Bilgi Güvenliği Politikasına uyum konusundaki isteklerini etkilediğini (Bulgurcu vd., 2010) ve yeni oluşturulan kimlik bilgilerinin şifre kalitesiyle farkındalık arasındaki korelasyonu (Mamonov ve Benbunan-Fich, 2018) ortaya koymuştur. Farkındalığın farklı bir yönünü tanıtan Li vd. (2019), çalışanların bir kuruluşun bilgi güvenliği politikasına ilişkin farkındalığının, bilgi güvenliği algılarını etkilediğini ve kendilerinin bildirdiği bilgi güvenliği koruma davranışlarını etkilediğini bulmuştur. Yakın zamanda yapılan bir çalışmada Donalds ve Osei-Bryson (2020), kimlik bilgileri

güvenliđi uyum eylemlerinin yanı sıra genel güvenlik uyumluluđu açısından güvenlik farkındalıđının etkisini gösteren somut kanıtlar sunmuştur.

Önceki çalışmayla uyumlu olarak önerimiz, çalışanların güvenlik farkındalıđı düzeyi arttıkça siber güvenlik uyum davranışı sergileme eğilimlerinin de arttığı yönündedir. Buradan hareketle;

H6: Çalışanların güvenlik farkındalıđının derecesi, siber güvenlik önlemlerine uyma davranışlarını olumlu yönde etkilemektedir.



3. YÖNTEM

Bu bölümde, yukarıda açıklanan yapılar ile çalışanlar arasındaki siber güvenlik uyum davranışı arasındaki ilişkiyi araştırmak için kullanılan metodolojik çerçeve özetlemektedir. Bu kapsamda; tez kapsamında uygulanan ölçekler, veri toplama sürecinin detayları, incelenen örnekleme ilişkin özellikler ve toplanan verilerden anlamlı çıktılar elde etmek için benimsenen analitik yaklaşım açıklanmaktadır.

3.1. Ölçekler

Katılımcılara sunulan anket, yerleşik literatürden alınan çok sayıda maddeyi içeren ölçekleri içermektedir. Anket kapsamında güvenlik farkındalığı, algılanan engel, yanıt etkinliği, öz yeterlik, algılanan savunmasızlık ve algılanan önem derecesi de dâhil olmak üzere çeşitli siber güvenlik yapıları bulunmaktadır. Katılımcılardan bu soruları yanıtlarken siber güvenlik davranışlarını dikkate almaları istenmiştir.

Ayrıca katılımcılara, karar verme tarzlarını belirlemek üzere Genel Karar Verme Tarzı Envanteri (GKVT) soruları yöneltilmiş ve bunları karar verme sürecinde kullandıkları yaklaşımları dikkate alarak yanıtlamaları istenmiştir.

Çalışmanın bağımlı değişkeni olan siber güvenlik uyum eylemleri, Ng vd. (2009), Anwar vd. (2017) ve Donalds ve Osei-Bryson'ın (2020) çalışmalarından alınan dört sorulu bir ölçek aracılığıyla ölçülmüştür. Algılanan önem derecesi, Woon vd. (2005), Ng vd. (2009), Mohamed ve Ahmad (2012), Ifinedo (2012) ve Li vd.'nin (2019) çalışmalarında kullanılan dört sorulu bir ölçek aracılığıyla ölçülmüştür. Bir diğer önemli unsur olan algılanan savunmasızlık, Woon vd. (2005), Ifinedo (2012) ve Li vd.'den (2019) alınan dört sorulu bir ölçek aracılığıyla ölçülmüştür. Bireylerin yeteneklerine olan inancını içeren öz yeterlik, Rhee vd. (2009), Anwar vd. (2017), Li vd. (2019) ve Donalds ve Osei-Bryson'dan (2020) alınan dört sorulu bir ölçek aracılığıyla ölçülmüştür. Önerilen karşı davranışların etkinliğini değerlendiren yanıt etkinliği, Lee vd. (2008), Mohamed ve Ahmad (2012) ve Li vd.'nin (2019) çalışmalarından alınan dört sorulu bir ölçek aracılığıyla ölçülmüştür. Potansiyel engelleri yansıtan algılanan engel, Woon vd. (2005), Ng vd. (2009), Anwar vd. (2017) ve Li vd. (2019) alınan dört sorulu bir ölçek aracılığıyla ölçülmüştür. Kritik bir boyut olan güvenlik farkındalığı Bulgurcu vd. (2010) ve Donalds ve Osei-Bryson'dan (2020)

alınan üç sorulu bir ölçek aracılığıyla ölçülmüştür. Son olarak, kişisel karar alma tarzı, Scott ve Bruce'un (1995) 25 soruluk kapsamlı Genel Karar Verme Tarzı Envanteri (GKVT) kullanılarak değerlendirilmiştir.

Orijinal dillerine uygun olarak aslen İngilizce olarak hazırlanan anket, uygulanmadan önce Türkçe'ye çevrilmiştir. İçerik ve görünüş geçerliliğini pekiştirmek maksadıyla, ana dilleri Türkçe olan üç farklı araştırmacı Türkçe ifadeleri incelemiş ve onların geri bildirimlerine dayanarak çevirilerde tekrar iyileştirmeler yapılmıştır.

Anketteki maddeler daha sonra katılımcılara (1) 'Hiçbir Zaman' ile (5) 'Her Zaman' arasında değişen beş seçenekli bir Likert ölçek ölçeğinde sunulmuştur. Katılımcılardan ayrıca eğitim düzeyi, yaş, cinsiyet, çalıştığı sektör gibi temel demografik veriler ve kurumlarında güvenlik bilgilerine ilişkin bir politikanın varlığına yönelik bilgi talep edilmiştir. Çalışmada kullanılan ölçeklerin boyut ve ifadelerine ilişkin detaylar Ek-A'da ayrıntılı olarak sunulmuştur.

3.2. Verilerin Toplanması ve Örnekleme Prosedürü

Verizon'un (2022) vurguladığı gibi, kuruluşlardaki siber güvenliğin temel taşı çalışanlardır. Sonuç olarak, bu çalışmanın katılımcılarını hem kamu hem de özel sektör çalışanlarının yanı sıra daha önce çalışma tecrübesi bulunan öğrenciler oluşturmaktadır. Farklı sektörlerden katılımcıların bu şekilde birleştirilmesi, Donalds ve Osei-Bryson (2020) tarafından da işaret edildiği gibi Bilgi Sistemleri araştırmalarındaki yaygın uygulamayla uyumludur. Tez kapsamında incelenen veriler, çalışanların siber güvenlik davranışları ile karar verme tarzları arasındaki karmaşık ilişkileri incelemek için geliştirilen bir anket kullanılarak toplanmıştır. Çevrimiçi anket tekniğinin kullanılması, farklı bölgelerden, kurumlardan ve demografik geçmişlerden veri toplanmasını kolaylaştırmış ve bakış açılarının kapsamlı bir şekilde temsil edilmesini sağlamıştır.

Tez çalışmasının her aşamasında etik hususlar dikkatle ele alınmıştır. Araştırmanın amaçlanan hedefleri anket öncesinde tüm katılımcılara şeffaf bir şekilde aktarılmış ve katılımcılara anket sorularını cevaplama aşamasında araştırmadan ayrılma seçeneği sunulmuştur. Araştırmaya katılım tamamen gönüllülük esasına dayanmakta olup katılımcılara cevaplarının anonimleştirileceği ve özel kalacağı konusunda güvence verilmiştir. Çalışma, Gebze Teknik Üniversitesi Akademik İnsan Araştırmaları Etik

Kurulu'ndan 2022/12-02 numaralı bildiriyle etik kurul onayı almıştır. Bahse konu onaya ilişkin dokümanlar **Ek-B'**de sunulmuştur.

Araştırma anketi, sırasıyla 31 ve 35 katılımcıyı içeren iki pilot araştırma çalışmasıyla test edilmiştir. Pilot çalışmaların ardından ankette iyileştirmeler yapılarak son hâli oluşturulmuştur. Veri temizliğinin ardından, veri setinde toplam 668 katılımcı yer almış ve anket süreci sonuç olarak %67'lik bir yanıt oranıyla sonuçlanmıştır. Kalan yanıtlar, Hair vd. (2006) ve Westland'ın (2010) çalışmalarında belirtildiği gibi sonraki veri analizi için uygun, güçlü bir örneklem boyutu oluşturmaktadır.

Tablo 3.1, katılımcının demografik ve sosyal bilgilerini özetlemekte olup aşağıda sunulmuştur;



Tablo 3.1: Örneklemin Demografik Yapısı (n=668).

Özellikler	N	%
<i>Cinsiyet</i>		
Kadın	386	57.8
Erkek	282	42.2
<i>Yaş</i>		
<=20	6	0,9%
21-25	164	24,5%
26-30	149	22,3%
31-35	175	26,1%
36-40	86	12,8%
41-45	53	7,9%
>46	35	5,2%
<i>Eğitim Seviyesi</i>		
Lise	31	4.7
Ön Lisans	30	4.5
Lisans	413	61.8
Yüksek Lisans	173	25.9
Doktora	21	3.1
<i>Sektör</i>		
Bilgi Teknolojisi ve Telekomünikasyon	34	5,1%
Sağlık	78	11,7%
Bankacılık / Finansal Hizmetler / Sigorta	17	2,5%
Emlak	3	0,4%
Perakende ve Toptan Satış	12	1,8%
Eğitim	216	32,3%
Hukuk Hizmetleri	16	2,4%
Askeri Hizmetler	83	12,4%
Turizm	3	0,4%
Diğerleri	206	30,8%
<i>Çalıştığınız kurumunuzun bilgi güvenliği konusunda bir politikası var mı?</i>		
Evet	383	57,3%
Hayır	73	10,9%
Bilmiyorum	212	31,7%

668 kişiden oluşan son grubun %57,8'i kadın, %26'sı 31-35 yaş aralığında ve %61,8'i lisans diplomasına sahip katılımcılardan oluşmaktadır. Ayrıca çalıştıkları kurumun bilgi güvenliği politikası olup olmadığına ilişkin soruya, %57,1'i "evet", %10,8'i

"hayır" yanıtını verirken, %31,9'u kurumun bilgi güvenliği politikasına ilişkin herhangi bir şeyden haberi olmadığını ifade etmiştir.

3.3. Veri Analizi

Verilerin analizinde SPSS yazılımı kullanılmıştır. Modelin bağımsız değişkenlerinin ölçeklerinin literatürde nispeten yeni olduğu göz önüne alındığında, bu değişkenlere ait faktörlerin bağımlı değişkenimiz olan siber güvenlik uyumluluğundaki fiilleri üzerindeki yüklerini değerlendirmek için döndürülmüş bir varimax temel bileşen incelemesi yapılmıştır. Bu prosedür, hem bağımsız değişkenler hem de sonuç değişkenleri için öğelerin tanımlanmasına yardımcı olmuştur.

Yapılan faktör analizini sonucu, siber güvenlik davranışlarını kapsayan yapılara ilişkin 27 ifade, yedi farklı gruba ayrılmıştır. Faktör analizi sonuçları, **Tablo 3.2**'de sunulmuştur;

Tablo 3.2: Faktör Analizi Sonuçları.

	Bileşenler						
	1	2	3	4	5	6	7
Algıl. Önem Derecesi_ PeSe-1	,778						
PeSe-2	,799						
PeSe-3	,818						
PeSe-4	,772						
Algıl. Savunmasızlık_PeVu-1						,622	
PeVu-2						,747	
PeVu-3						,604	
PeVu-4						,599	
Öz Yeterlik_SEfe-1		,831					
SEfe-2		,888					
SEfe-3		,858					
SEfe-4		,798					
Yanıt Etkinliği_REfe-1			,670				
REfe-2			,786				
REfe-3			,753				
REfe-4			,673				
Algılanan Engel_PeBa-1					,860		
PeBa-2					,881		
PeBa-3					,800		
PeBa-4					,495		
Güvenlik Farkındalığı_SeAw-1							,759
SeAw-2							,755
SeAw-3							,662
Sib.Güv.Uyum Dav. _CCB-1				,674			
CCB-2				,658			
CCB-3				,864			
CCB-4				,856			

Bireylerin karar verme tarzlarını ölçmek amacıyla kullanılan Genel Karar Verme Tarzı Envanteri (GKVT), literatürde bilinen ve sık kullanılan bir ölçek olduğundan faktör analizine gerek duyulmamıştır.

Araştırmada her bir değişken için Cronbach alfa değerleri 0,77 ile 0,91 arasında değişmektedir. Bilindiği üzere, 0,70'in üzerindeki bir güvenirlik katsayısı olumlu kabul edilir (DeVellis, 2003). Dolayısıyla bu çalışmada tüm değişken ölçümleri için elde edilen Cronbach alfa değerleri yüksek güvenirliğin göstergesidir.



4. BULGULAR

Regresyon analizleri, siber güvenlik davranışlarını açıklamak amacıyla bireylerin karar verme tarzlarına odaklanarak yürütülmüştür. Bu kapsamda öncelikle tüm katılımcıları içeren genel grup üzerinde, sonrasında bireysel karar verme tarzları bakımında birbirinden farklılaşan alt gruplar özelinde regresyon analizleri yapılmıştır.

Başlangıçta, tanımlayıcı istatistiksel veriler ve yedi yapı arasındaki maddeler arası korelasyonlar incelenmiştir. Ortalama değerlerin, standart sapmaların ve değişkenler arasındaki korelasyonların bir özeti **Tablo 4.1**'de özetlenmiştir;

Tablo 4.1: Korelasyonlar.

	Ort.	SS.	CrAlph	1	2	3	4	5	6
1 PeSe	4,56	,72	,91						
2 PeVu	4,28	,80	,89	,713**					
3 SEfe	3,31	1,04	,90	,262**	,352**				
4 REfe	4,23	,76	,87	,655**	,749**	,370**			
5 PeBa	2,79	,99	,77	-,016	,040	,117**	,050		
6 SeAw	3,83	,88	,81	,420**	,513**	,521**	,582**	,109**	
7 CCB	3,92	,91	,85	,459**	,479**	,382**	,490**	,078*	,500**

** $P < 0,01$

* $P < 0,05$

Daha sonra, varsayılan ilişkileri değerlendirmek için regresyon yöntemleri kullanılarak istatistiksel analizler yapılmıştır. İlk regresyonun analizi, katılımcıların karar verme tarzlarına bakılmaksızın tüm grubu kapsamaktadır.

Genel grup için **Tablo 4.2**'de gösterildiği gibi, güvenlik farkındalığı ($\beta = 0,238$; $p < 0,01$), yanıt etkinliği ($\beta = 0,106$; $p < 0,05$), öz yeterlik ($\beta = 0,133$; $p < 0,01$), algılanan savunmasızlık ($\beta = 0,096$; $p < 0,05$) ve algılanan önem derecesi ($\beta = 0,186$; $p < 0,01$) siber güvenlik uyum davranışıyla pozitif ilişkiler göstermiştir;

Tablo 4.2: Genel Regresyon Analizi Sonuçları.

Model 1			
Bağımlı Değişken: CCB			
	Beta	t	Sig.
PeSe	,186	4,014	,000**
PeVu	,096	1,809	,026*
SEfe	,133	3,588	,000**
REfe	,106	2,052	,020*
PeBa	,030	,962	,118
SeAw	,238	5,635	,000**
R^2		,356	
F		60.823	
$Sig.$		.000	

** $P < 0,01$

* $P < 0,05$

Yukarıda sunulmuş olan Model-1 incelendiğinde, algılanan engel ile siber güvenlikteki uyum davranışı arasında beklenen ampirik bağlantının sağlanamadığı görülecektir. Model-1, veri seti ile önemli bir istatistiksel uyum sergileyerek ($R^2 = 0,356$, $F = 60,823$, $p = 0,000$), siber güvenlik uyum davranışındaki değişimin %35,6'sını açıklamıştır. Sonuç olarak; H1, H2, H3, H4 ve H6 destek alırken H5, bireylerin karar verme tarzlarına bakılmaksızın tüm katılımcılar için desteklenememiştir.

Daha sonra bireysel karar verme tarzları bakımından farklılaşan katılımcı alt grupları için (rasyonel, sezgisel ve bağımlı tarzlar) ayrı ayrı regresyon analizleri yapılmıştır. Anımsanacağı üzere veri setinde, iki karar verme tarzı için (kaçınma ve spontane tarzlar) yeterli miktarda örneklem gözlenmemiştir. Bununla birlikte, bu çalışmada analiz edilen karar verme tarzları, Harren'in (1979) bağımlı, sezgisel ve rasyonel karar verme tarzlarını kapsayan ve literatürde sıkça kullanılan sınıflandırmasından alınmıştır.

Rasyonel karar verme tarzına sahip bireylere ilişkin regresyon analizi sonuçları **Tablo 4.3'**te sunulmuştur;

Tablo 4.3: Rasyonel Karar Verme Tarzına Sahip Bireyler İçin Regresyon Analizi Sonuçları.

Model 2			
Bağımlı Değişken: CCB			
	Beta	t	Sig.
PeSe	,200	3,720	,000**
PeVu	,094	1,449	,148
SEfe	,153	3,104	,002**
REfe	,096	1,497	,135
PeBa	,017	,400	,689
SeAw	,198	3,577	,000**
R^2		,303	
F		28.875	
$Sig.$		.000	

** $P < 0,01$

* $P < 0,05$

Rasyonel karar verme tarzına sahip bireyler için güvenlik farkındalığı ($\beta = 0,198$; $p < 0,01$), algılanan önem derecesi ($\beta = 0,200$; $p < 0,01$) ve öz yeterlik ($\beta = 0,153$; $p < 0,01$) siber güvenlik uyum davranışı ile pozitif korelasyonlar göstermiştir.

Genel durumu temsil eden Model-1 sonuçlarının aksine, rasyonel karar verme tarzına sahip bireylerin durumlarını tasvir eden Model-2 kapsamında, siber güvenlik uyum davranışı ile algılanan savunmasızlık ve yanıt etkinliği arasındaki bağlantıları destekleyecek bir kanıt bulunamamıştır. Benzer şekilde karar vermede rasyonel tarza sahip bireyler için, Model-1'de gözlemlenen duruma paralel olarak, engel algısı ile siber güvenlik uyum davranışı arasındaki bağlantıya dair ampirik bir kanıt gözlemlenmemiştir. Model-2, veri seti ile anlamlı bir istatistiksel uyum göstermiş ($R^2 = 0,303$, $F = 28,875$, $p = 0,000$) ve siber güvenlik uyum davranışındaki değişimin %30,3'ünü açıklamıştır. Dolayısıyla H1, H3 ve H6 istatistiksel olarak desteklenirken, H2, H4 ve H5 karar vermede rasyonel tarza sahip olan bireyler özelinde desteklenmemektedir.

Tablo 4.4'te sezgisel karar verme tarzına sahip bireylerin kategorisine ilişkin regresyon analizi sonuçları sunulmuştur;

Tablo 4.4: Sezgisel Karar Verme Tarzına Sahip Bireyler İçin Regresyon Analizi Sonuçları.

Model 3			
Bağımlı Değişken: CCB			
	Beta	t	Sig.
PeSe	-,003	-,023	,982
PeVu	,193	1,345	,182
SEfe	,097	1,205	,231
REfe	,231	1,797	,027*
PeBa	-,027	-,390	,697
SeAw	,339	3,461	,001**
R^2		,540	
F		20,573	
$Sig.$		.000	

** $P < 0,01$

* $P < 0,05$

Sezgisel karar vericiler için, güvenlik farkındalığının ($\beta = 0,339$; $p < 0,01$) ve yanıtın etkinliğinin ($\beta = 0,231$; $p < 0,05$) siber güvenlik uyum davranışıyla pozitif yönde ilişkili olduğu gözlemlenmiştir. Ancak algılanan önem derecesi, algılanan savunmasızlık, öz yeterlik ve algılanan engel ile siber güvenlik uyum davranışı arasındaki ilişkiler Model-3 tarafından desteklenmemiştir. Model-3, veri seti ile önemli bir istatistiksel eşleşme göstererek siber güvenlik uyum davranışındaki değişimin %54'ünü açıklamıştır. Dolayısıyla H4 ve H6 istatistiksel olarak desteklenirken H1, H2, H3 ve H5 sezgisel karar verme tarzına sahip bireyler için desteklenmemektedir.

Tablo 4.5'te bağımlı karar verme tarzına sahip bireylerin kategorisine ilişkin regresyon analizi sonuçları sunulmuştur;

Tablo 4.5: Bağımlı Karar Verme Tarzına Sahip Bireyler İçin Regresyon Analizi Sonuçları.

Model 4			
Bağımlı Değişken: CCB			
	Beta	t	Sig.
PeSe	,236	1,468	,145
PeVu	,255	1,593	,110
SEfe	,079	,793	,430
REfe	-,046	-,293	,770
PeBa	,135	1,592	,110
SeAw	,199	1,713	,045*
R^2		,397	
F		10,303	
$Sig.$		.000	

** $P < 0,01$

* $P < 0,05$

Tablo 4.5'te görüleceği üzere, bu grup için yalnızca güvenlik farkındalığının ($\beta = 0,199$; $p < 0,05$) siber güvenlik uyum davranışı ile pozitif bir ilişki sergilediği görülmüştür. Siber güvenlikte algılanan önem derecesi, algılanan savunmasızlık, öz yeterlik, yanıtın etkinliği ve algılanan engel ile siber güvenlik uyum davranışı arasındaki ilişkiler desteklenmemiştir. Model-4, veri setiyle anlamlı bir istatistiksel uyum göstermiş ($R^2 = 0,397$, $F = 10,303$, $p = 0,000$) ve siber güvenlik uyum davranışındaki değişimin %39,7'sini açıkladı. Sonuç olarak sadece H6 destek alırken, H1, H2, H3, H4 ve H5 karar vermede bağımlı tarza sahip olanlardan destek bulamamıştır.

Tablo 4.6, tüm regresyon analizlerinin sonuçlarını özetlemektedir;

Tablo 4.6: Regresyon Analizleri Özeti.

	Model 1 Bağımlı Değ. CCB GENEL			Model 2 Bağımlı Değ. CCB RASYONEL KVT			Model 3 Bağımlı Değ. CCB SEZGİSEL KVT			Model 4 Bağımlı Değ. CCB BAĞIMLI KVT		
	Beta	t	Sig.	Beta	T	Sig.	Beta	t	Sig.	Beta	t	Sig.
PeSe	,186	4,014	,000**	,200	3,720	,000**	-,003	-,023	,982	,236	1,468	,145
PeVu	,096	1,809	,026*	,094	1,449	,148	,193	1,345	,182	,255	1,593	,110
SEfe	,133	3,588	,000**	,153	3,104	,002**	,097	1,205	,231	,079	,793	,430
REfe	,106	2,052	,020*	,096	1,497	,135	,231	1,797	,027*	-,046	-,293	,770
PeBa	,030	,962	,118	,017	,400	,689	-,027	-,390	,697	,135	1,592	,110
SeAw	,238	5,635	,000**	,198	3,577	,000**	,339	3,461	,001**	,199	1,713	,045*
R^2	,356			,303			,303			,303		
F	60.823			28.875			28.875			28.875		
$Sig.$	.000			.000			.000			.000		

*** $P < 0,01$ * $P < 0,05$

5. ARAŞTIRMA SONUÇLARININ YORUMLANMASI

Bu tez, çalışanların karar verme tarzlarındaki farklılıkların siber güvenlikteki mevcut uyumluluk eylemlerini nasıl etkilediğini inceleyerek siber güvenlik uyum davranışının anlaşılmasına yeni bakış açıları katmaktadır. Bu bağlamda, bulgular iki açıdan değerlendirilebilir: birincisi, modeli tüm katılımcıları kapsayan grubun tamamı için değerlendirilmesi ve ikinci olarak, siber güvenlikteki mevcut uyumluluk eylemlerinin, insanların karar verme tarzlarına göre karakterize edilen alt bölümler arasındaki farklılıkları incelenmesi.

Güvenlik farkındalığının, yanıt etkinliğinin, öz yeterliğin, algılanan önem derecesinin ve algılanan savunmasızlığın tüm örneklem için siber güvenlikle ilgili uyumluluk eylemlerini etkilediği ancak algılanan engel yapısının etkisinin bulunmadığı bulunmuştur. Tüm değişkenlerin etkisinin genel grup ve alt bölümlere göre değiştiği gözlemlenmiştir. Ancak algılanan engel yapısının için hiçbir alt bölüm üzerinde önemli bir tanımlayıcı etkisi bulunmazken, güvenlik farkındalığı hem genel örneklemde hem de alt bölümlerin tamamında kritik bir açıklayıcı parametre olarak ortaya çıkmıştır.

Çalışanların algılanan önem dereceleri ile siber güvenlik alanındaki uyum eylemleri arasında ilişki incelenmiş ve bu iki yapı arasında pozitif bir bağlantı olduğu sonucuna ulaşılmıştır. Bu bulgular, Mohamed ve Ahmad (2012), Mohamed ve Ahmad (2012), Vance vd. (2012), Bulgurcu vd. (2010), Pahnla vd. (2007) ve Larose vd.'nin (2005) sonuçlarıyla uyumludur.

Sonuçlar karar verme tarzı açısından incelendiğinde, algılanan önem derecesinin, karar vermede rasyonel tarza sahip bireylerin siber güvenlik konusundaki uyum eylemlerini güçlü bir şekilde açıkladığı, sezgisel ve bağımlı tarza sahip bireylerin davranışlarını ise açıklayamadığı görülmüştür.

Muhtemel siber saldırıların algılanan önem derecesinin siber güvenlik uyum davranışı üzerindeki açıklayıcı etkisinin bulunması daha önceki bazı araştırmalarla kısmen çelişmektedir. Örneğin Ng vd. (2009) tarafından yürütülen çalışmada, aynı yapıları arasında ilişki tespit edilememiş, bu durum ise insanların siber uzaydan kaynaklanan

olası riskler konusunda farkındalık eksikliğine bağlanmıştır. Ng vd. (2009) tarafından tespit edilemeyen bu ilişkiye dair yapılan değerlendirme, karar vermede bağımlı ve sezgisel tarza sahip çalışanların, rasyonel kararlar veren kişilere kıyasla siber güvenlik konusunda daha az farkındalık sergilediğini ortaya koyarak doğrulanmıştır.

Çalışanların algılanan savunmasızlığı ile siber güvenlik uyum eylemleri arasındaki ilişki incelendiğinde, pozitif bir ilişki olduğu gözlemlenmiştir. Bu tespit, Li vd. (2019), Anwar vd. (2017) ve Ifinedo'nun (2012) bulgularıyla uyumlu olup Lee vd. (2008) tarafından yapılan çalışmayı da çalışan örnekleminin incelenmesi bakımından genişletmiştir.

Ancak katılımcılar bir bütün olarak ele alındığında bu olumlu ilişki belirgin iken, karar verme tarzlarına göre alt bölümlere göre incelendiğinde bu ilişkinin devam etmediği görülmektedir. Katılımcı sayısının azalmasıyla olumlu ilişki azalmıştır. Workman vd. (2008) benzer şekilde, savunmasızlığın çalışanların bilgi güvenliği önlemlerini gözden kaçırma potansiyelini açıklamada çok önemli bir faktör olmasına rağmen, bu etkileri gösteren katsayıların dikkate alınamayacak kadar az kabul edildiğini belirtmiştir.

Tez çalışması kapsamında yapılan analizler, önceki çalışmalarla uyumlu olarak siber güvenlikte uyumluluk eylemlerini açıklamada bireylerin öz yeterliliğinin önemini ortaya çıkarmıştır (Li vd., 2019; D'Arcy ve Lowry, 2019; Bulgurcu vd., 2010; Ng vd., 2009). Sonuçlar, karar tarzları bağlamında öz yeterliğin, karar vermede rasyonel tarza sahip bireylerin siber güvenlik konusundaki uyum eylemlerine önemli ölçüde katkıda bulunduğunu göstermiştir. Ancak bağımlı ve sezgisel tarza sahip olanların karar vermedeki eylemlerini tam olarak açıklayamamıştır. Öz yeterliğin rolüne benzer şekilde Ameen vd. (2020), kültürler arasında akıllı telefon güvenliği davranışsal niyetinde cinsiyet farklılıklarını açıklayan çalışmalarında karışık sonuçlar bildirmişlerdir. Bulguları, öz yeterliliğin ABD'deki kadınların davranışsal niyetlerini önemli ölçüde etkilediğini, BAE'deki hem erkekler hem de kadınlar arasında ihmal edilebilir bir etkiye sahip olduğunu göstermiştir. Bununla birlikte, çalışmaların çoğuyla tutarlı olarak bu tez, çalışanların siber güvenlik konusundaki uyum faaliyetlerinde öz yeterliğin temel rolünün altını çizmektedir.

Çalışanların yanıt etkinliği ile siber güvenlik uyum eylemleri arasında ilişkinin incelenmesi, önceki çalışmalarla tutarlı olarak bu ilişkinin önemini ortaya çıkarmıştır (Li vd, 2019; Vance vd., 2012; Lee ve Larsen, 2009; Herath ve Rao, 2009a). Sonuçlar,

karar verme tarzları bakımından, yanıt etkinliğinin, sezgisel tarza sahip bireylerin karar vermedeki eylemlerini açıkladığını, ancak rasyonel ve bağımlı tarza sahip olanların karar vermedeki eylemlerini tam olarak açıklamadığını göstermiştir. Bu farklılık, karar vermede sezgisel tarza sahip çalışanların, duygulara dayalı bir seçim yapma eğiliminin daha fazla olması ve yanıtlarının etkililiğine olan güvenin artmasından kaynaklanıyor olabilir.

Siber güvenlik alanında çalışanların uyum eylemleri üzerindeki algılanan engel etkilerinin analizi, çalışmamızda önemli bir etki ortaya çıkarmamıştır. Bu etki eksikliği, ne grubun tamamında ne de karar verme tarzlarına göre alt bölümlerde gözlemlenmemiştir. Algılanan engel, siber güvenlik alanında uyum eylemlerinin gerçekleştirilmesiyle ilişkili kaygı veya rahatsızlık anlamına gelir. Sonuç olarak bu ilişki eksikliği, katılımcıların karar verme tarzlarında siber güvenlik koruma davranışlarına katılımlarını engelleyen önemli engeller algılamadıkları şeklinde yorumlanabilir.

Çalışmamızda güvenlik farkındalığının çalışanların siber güvenlik uyum davranışını etkileyen önemli bir faktör olduğu ortaya çıkmış; bu durum ise bilgili bireylerin siber güvenlik düzenlemelerine uymaya daha yatkın olduğu hipotezimizi doğrulamıştır. Bu sonuçlar, Li vd. (2019) ve Donalds ve Osei-Bryson'nın (2020) sonuçlarıyla tutarlılık sergilemiştir. Bu tez, bir kuruluştaki bilgi güvenliğine ilişkin bir politikanın varlığına ilişkin farkındalığın ötesine geçerek, güvenlik farkındalığı için kapsamlı bir ölçek kullanarak Li vd. (2019) çalışmasını tespitlerini genişletmektedir. Ayrıca araştırmamız, alternatif bir karar verme tarzı değerlendirmesi olan Genel Karar Verme Tarzı Envanterinin (GKVT) kullanılması ile Donalds ve Osei-Bryson'un (2020) çalışmasının kapsamını genişletmektedir.

Bulgular, güvenlik farkındalığının, bağımlı, sezgisel ve rasyonel karar vericileri kapsayan tüm karar verme tarzı alt bölümlerinde çalışanların siber güvenlik konusundaki uyumluluk eylemlerini açıklayan tek önemli bileşen olduğunu göstermektedir. Ancak alt gruplar güvenlik farkındalığı açısından önem düzeyi açısından değerlendirildiğinde, karar vermede rasyonel, sezgisel ve bağımlı tarzlar sırası ile sıralanmaktadır. Bu sonuçlar, Donalds ve Osei-Bryson'un (2020) bir kişinin baskın karar tarzının, güvenliğe uyum eylemleri üzerinde büyük bir etkiye sahip olduğu iddiasına ampirik destek sunmaktadır.

Tezin teorik ve pratik katkıları aşağıda iki ayrı alt bölüm hâlinde aşağıdaki bölümlerde detaylandırılmıştır.

5.1. Teorik Katkılar

Bu tez, siber güvenlik araştırmaları alanına üç önemli teorik katkı sunmaktadır.

İlk olarak, Karar Verme Tarzı ve Koruma Motivasyonunun teorik yapısına dayanan bu tez, bireylerin siber güvenlikteki uyum eylemlerini anlamada karar verme tarzı farklılıklarının alınmasında tarzların önemli rolünü vurgulayan bir araştırma modelini sunmakta ve doğrulamaktadır.

İkinci olarak, önerilen ve doğrulanan araştırma modeli, özellikle sınırlı sayıda çalışmaya ampirik kanıt sağlaması bakımından, siber güvenlikte uyum eylemlerine ilişkin karar verme tarzlarının etkisinin araştırılmasında mevcut literatüre kayda değer bir katkı sağlamaktadır (Donalds ve Osei-Bryson, 2020; Gratian vd., 2018; Egelman ve Peer, 2015).

Son olarak bu tez, literatürdeki yaygın davranışsal niyetlere odaklanmanın aksine, çalışanların siber güvenlik alanındaki somut uyum eylemlerini incelemektedir. Gelecekteki davranışlara ilişkin beklentiler yerine, kişisel olarak rapor edilmiş olsalar bile gerçek eylemlerin vurgulanması, günlük yaşamda daha bilinçli önlemlerin alınması açısından önem arz etmektedir. Gerçek davranışlara yapılan bu vurgu, somut eylemlerin ve yanıtların dijital savunmaları güçlendirmede önemli bir rol oynadığı siber güvenliğin karmaşıklıklarıyla baş etmede özellikle geçerli hale gelmektedir. Tez kapsamında gözlemlenen davranışlara odaklanarak, teorik varsayımların ötesine geçilmekte ve siber güvenlik uyumluluğunun pratik yönlerini inceleyerek, sürekli gelişen dijital güvenlik ortamında çalışanların eylemlerini etkileyen faktörlerin daha ayrıntılı bir şekilde araştırılmasına olanak sağlanmaktadır.

5.2. Uygulamaya Yönelik Katkıları

Siber güvenlik uyum eylemlerine ilişkin çalışanların karar verme tarzlarının etkisini anlamak, kuruluşlar içinde daha etkili güvenlik önlemlerinin uygulanması açısından oldukça önemlidir. Çalışanlar arasındaki bireysel farklılıkların, özellikle de karar verme tarzlarının farkında olan bir yönetici, potansiyel güvenlik açıklarını proaktif bir

şekilde ele alabilir. Bu anlayıştan yararlanılarak bu farklılıklar kurumsal avantajlara bile dönüştürülebilir.

Çalışanların karar verme tarzlarındaki farklılıkların belirlenmesi, yöneticilerin bireyleri, belirli özelliklerine uygun rollere stratejik olarak atamasını sağlar. Örneğin rasyonel karar verme tarzına sahip çalışanlar, güvenlik duvarı, Saldırı Önleme Sistemi (IPS), Web Uygulama Güvenlik Duvarı (WAF) yönetimi gibi organizasyon için kritik öneme sahip teknik rollere yönlendirilebilir. Bunu yaparken, farklı şekillerde karar verenlerin aksine, bu rollerdeki çalışanlar için güvenlik farkındalığı, öz yeterlik ve algılanan önem derecesi gibi faktörler daha belirgin hale gelmektedir. Alternatif olarak bu tür pozisyonlara alım yapılırken, bu eğilimleri gösteren adayların tercih edilmesi vurgulanabilir. Bu hedefe yönelik yaklaşım, belirli karar verme tarzlarına sahip bireylerin, güçlü yönlerine ve tercihlerine en uygun rollere uyum sağlamalarının optimize edilmesine yardımcı olacaktır.

Benzer şekilde, karar vermede sezgisel tarzlara sahip teknik personel, Bilgisayar Güvenliği Olay Müdahale Ekibine (CSIRT) katkıda bulunmak veya Güvenlik Bilgileri ve Olay Yönetimi (SIEM) sistemini denetlemek gibi siber tehditlere hızlı yanıt gerektiren rollerde stratejik olarak konumlandırılmalıdır. Sezgisel karar verme tarzlarının yanıt etkinliği faktörünün siber güvenlikteki uyum eylemlerini etkilediği göz önüne alındığında, karar vermede bu tarza sahip bireylerin potansiyel tehditleri engellemede başarılı olmaları beklenmektedir. Çalışanlara kişilik özelliklerini, özellikle de karar verme tarzlarını tamamlayan roller vermek, kurumsal siber güvenliğin artırılmasına önemli bir katkı sağlamaktadır.

5.3. Araştırmanın Kısıtları ve Önerileri

Koruma Motivasyonu Teorisi perspektifinden siber güvenlik alanında çalışanların karar verme tarzları ve uyumluluk eylemleri arasındaki ilişkiye dair değerli bilgiler sağlarken, bu çalışma gelecekteki araştırma çabalarının önünü açan bazı sınırlamaları da barındırmaktadır.

İlk olarak, gelecekteki araştırmalar, oyundaki karmaşık dinamiklere dair anlayışımızı zenginleştirmek için Nötrleştirme Teorisi, Planlı Davranış Teorisi, Genel Caydırıcılık Teorisi veya Rasyonel Seçim Teorisi gibi güvenlikle ilgili çeşitli kavramsal yapıları kullanarak benzer bir bağlantıyı keşfedebilir.

İkinci olarak, Scott ve Bruce'un (1995) Genel Karar Verme Tarzı Envanterinin (GKVT) bu tezde kullanılması, gelecekteki arařtırmalar için aynı anketin alternatif kavramsal yapılara dayanan çeřitli kavramsal modeller içinde kullanılmasına yönelik fırsatlar sunmaktadır. Ek olarak, Karar Tarzı Envanteri (Rowe ve Mason, 1987) gibi alternatif anketlerin kullanılması, karar tarzlarına ilişkin farklı bakıř açıları sunabilir.

Üçüncüsü, bu çalışma bağımlı deęiřken olarak bireylerin kendilerinin bildirdięi mevcut siber güvenlik uyum davranıřlarına dayansa da gelecekteki çalışmalar, siber güvenlik uyumluluęunun daha kapsamlı bir deęerlendirmesini mümkün kılacak řekilde davranıřları doęrudan gözlemlemeye yönelik önlemlerin iyileřtirilmesini düşünebilir.

Son olarak, bu tez için veri setinin toplandıęı spesifik coęrafi ve kültürel bağlam göz önüne alındıęında, gelecekteki araştırma çabaları, bulguların genellenebilirlięini artırmak ve daha kapsamlı bir yaklařım sunmak için çeřitli çok kültürlü, coęrafi ve sosyal ortamlardan bir veri seti derleyebilir.

6. SONUÇ

Kamu ve ticari sektördeki işletmelerin siber uzaydaki dayanıklılıklarını güçlendirmek için ortaya koyduğu önemli harcamalara rağmen, çalışanların bilgi güvenliği politikalarına uyma konusundaki isteksizliği veya başarısızlığı, kurumsal bilgi varlıklarının bütünlüğü açısından önemli bir risk oluşturmaktadır.

Siber güvenliği sağlamanın kritik bir bileşeni, çalışanların ilgili kurumların zorunlu kıldığı güvenlik düzenlemelerine uymasını gerektirir. Mevcut literatürde bireylerin siber güvenlik uyum davranışlarını açıklamaya yönelik çeşitli teorilere dayanan çok sayıda model yer alırken, bu çalışmaların önemli bir kısmında ağırlıklı olarak dış faktörlere vurgu yapılmış, bireylerin iç dinamikleri göz ardı edilmiştir. Belirlenen bu boşluğu gidermek amacıyla bu tez, içsel bir faktör olan bireylerin karar verme tarzlarının, çalışanların siber güvenlik uyum davranışlarını şekillendiren unsurlar üzerindeki etkisini incelemeyi amaçlamaktadır. Bu hedefe ulaşmak için, Koruma Motivasyonu Teorisine dayanan kavramsal bir model önerilmiş ve ampirik olarak test edilmiştir.

Bu tezin sonuçları, modelimizin bireylerin siber güvenliğe uyum davranışlarını etkili bir şekilde açıkladığını ve alt gruplar arasında karar verme tarzlarına bağlı olarak önemli farklılıklar olduğunu ortaya koymaktadır.

Tüm katılımcılardan oluşan genel grup için, güvenlik farkındalığı, yanıt etkinliği, öz yeterlik, algılanan savunmasızlık ve algılanan önem derecesi gibi faktörler, çalışanların siber güvenlik konusundaki uyumluluk eylemlerini önemli ölçüde etkilediği gözlemlenmiştir. Ancak algılanan engel faktörü için beklenen etki tespit edilememiştir. Bulguların derinliklerine inildiğinde, siber güvenlik farkındalığının, hem katılımcıların tamamı hem de tüm alt bölümler için, siber güvenlikte uyumluluk eylemlerini anlama konusunda karar verme tarzları açısından önemli bir belirleyici olduğu ortaya çıkmaktadır. Bununla birlikte, algılanan önem derecesi, algılanan savunmasızlık, öz yeterlik ve yanıt etkinliği etkileri, karar verme tarzlarına göre değişmektedir.

Özetlemek gerekirse; bu tez, Koruma Motivasyonu Teorisinin siber güvenlik davranışını anlamak için yararlı bir yapı sunduğuna dair önceki kanıtları

güçlendirirken aynı zamanda insanların siber güvenlik eylemlerine ilişkin karar verme tarzlarının etkisini de ortaya koymaktadır. Tez çalışması kapsamında yapılan yayın (Duzenci vd., 2023) ile birlikte bu tez, bireylerin içsel faktörlerinden biri olan karar verme tarzlarının siber güvenlik uyum davranışı üzerindeki etkisini incelemesi bakımından önem arz etmektedir. Bulgular, siber dayanıklı bir ortam oluşturmayı ve geliştirmeyi amaçlayan kuruluşlar için pratik çıkarımlar sağlamaktadır.



KAYNAKLAR

Ameen, N., Tarhini, A., Shah, M. H., and Madichie, N. O., (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, 104, 106184.

Allwood, C. M., Salo, I., (2012). Decision-making styles and stress, *International Journal of Stress Management*, 19(1), 34.

Anderson, C. L., Agarwal, R., (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 613-643.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443.

Appelt, K. C., Milch, K. F., Handgraaf, M. J., Weber, E. U., (2011). The Decision Making Individual Differences Inventory and guidelines for the study of individual differences in judgment and decision-making research. *Judgment and Decision Making*, 6(3), 252-262.

Barlow, J. B., Warkentin, M., Ormond, D., Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security*, 39, 145-159.

Bavolar, J., Orosova, O., (2015). Decision-making styles and their associations with decision-making competencies and mental health. *Judgment and Decision Making*, 10(1), 115-122.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., Polak, P., (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., Boss, R. W., (2009). If someone is watching, i'll do what i'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18, 151–164.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548.

Burns, A. J., Posey, C., Roberts, T. L., Lowry, P. B., (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 68, 190-209.

Chen, Y., Ramamurthy, K., Wen, K.-W., (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, 29(3), 157–188.

Crossler, R. E., Belanger, F., (2014). An extended perspective on individual security behaviors: Protection motivation theory and a Unified Security Practices (USP) instrument. *DATA BASE for Advances in Information Systems*, 45(4), 51–71.

Cybersecurity Ventures, <https://cybersecurityventures.com/cybersecurity-spending-2021-2025/>. Erişim Tarihi: 22.11.2023

D'Arcy, J., Lowry, P. B., (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43-69.

DeVellis, R. F., (2003), “Scale development: Theory and applications”, Thousand Oaks, CA: Sage Publications, Inc.

Donalds, C., Osei-Bryson, K. M., (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, 102056.

Driver, M. J., (1979). Individual decision-making and creativity. In: S. Kerr, Editor, “Organizational Behavior”, Columbus, OH: Grid Publishing.

Duzenci, A., Kitapci, H., Gok, M. S., (2023). The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior. *Applied Sciences (Switzerland)*, 13(15), 8731.

Egelman, S., Peer, E., (2015). “Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS)”, Proceedings of the 33rd annual ACM Conference on Human Factors in Computing Systems, 2873-2882, Seoul, Republic of Korea, 18–23 April.

Galotti, K. M., (2007). Decision structuring in important real-life choices. *Psychological Science*, 18(4), 320-325.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A., (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345-358.

Hadlington, L., (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346.

Han, J., Kim, Y. J., Kim, H., (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 66, 52-65.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., Tatham, R. L., (2006). “Multivariate Data Analysis”. New Jersey, Pearson Prentice Hall.

Harren, V. A., (1979). A model of career decision making for college students. *Journal of Vocational Behavior*, 14(2), 119-133.

Hazari, S., Hargrave, W., Clenney, B., (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy and Security*, 4(4), 3-20.

Herath, T., Rao, H. R., (2009a). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125.

Herath, T., Rao, H. R., (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Hovland, C. I., Janis, I. L., Kelley, H. H., (1953). “Communication and persuasion”, Yale University Press.

Hu, Q., Xu, Z., Dinev, T., Ling, H., (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6), 54–60.

Hunt, R. G., Krzystofiak, F. J., Meindl, J. R., Yousry, A. M., (1989). Cognitive style and decision making, *Organizational Behavior and Human Decision Processes*, 44(3), 436-453.

Ifinedo, P., (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.

Ifinedo, P., (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, 51(1), 69–79.

Janis, I. L., (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. *Advances in Experimental Social Psychology*, 3, 166-224.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., Wei, K.-K., (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*, 23(2), 139–154.

Kozhevnikov, M. (2007). Cognitive styles in the context of modern psychology: toward an integrated framework of cognitive style. *Psychological Bulletin*, 133(3), 464.

Larose, R., Rifon, N., Liu, S., Lee, D., (2005), “Understanding online safety behavior: A multivariate model”, The 55th annual conference of the international communication association, New York, NY, USA, 26–30 May.

Lee, D., Larose, R., Rifon, N., (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445-454.

Lee, Y., Larsen, K. R., (2009). Threat or coping appraisal: determinants of SMB executives’ decision to adopt anti-malware software. *European Journal of Information Systems*, 18(2), 177-187.

Lee, S. M., Lee, S. G., Yoo, S., (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, 41(6), 707-718.

Leering, A., van de Wijngaert, L., Nikou, S., (2022). More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors. *Behaviour & Information Technology*, 41(3), 519-534.

Leventhal, H., (1970). Findings and theory in the study of fear communications. *Advances in Experimental Social Psychology*, 5, 119-186.

Leykin, Y., DeRubeis, R. J., (2010). Decision-making styles and depressive symptomatology: Development of the Decision Styles Questionnaire. *Judgment and Decision Making*, 5(7), 506-515.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X., (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13–24.

Loo, R., (2000). A psychometric evaluation of the general decision-making style inventory. *Personality and Individual Differences*, 29, 895–905.

Lu, Y., (2018). Cybersecurity research: A review of current research topics. *Journal of Industrial Integration and Management*, 3(4).

Mamonov, S., Benbunan-Fich, R., (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, 83, 32-44.

Mann, L., (1982). Decision making questionnaires I and II. Unpublished questionnaires. *The Flinders University of South Australia*.

Mau, W. C., (2000). Cultural differences in career decision-making styles and self-efficacy. *Journal of Vocational Behavior*, 57(3), 365-378.

Messick, S., Fritzky, F. J., (1963). Dimensions of analytic attitude in cognition and personality 1, *ETS Research Bulletin Series*, 1963(1).

Mohamed, N., Ahmad, I. H., (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28, 2366–2375.

Moody, G. D., Siponen, M., Pahnla, S., (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 285–311.

Ng, B. Y., Kankanhalli, A., Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825.

Norman, P., Boer, H., Seydel, E. R., Mullan, B., (2015). “Protection Motivation Theory”, In: Conner, M., Norman, P., Editors, “Predicting and changing health behaviour: Research and Practice with Social Cognition Models”, Open University Press.

Nygren, T. E., (1997). Framing of task performance strategies: Effects on performance in a multiattribute dynamic decision making environment. *Human Factors*, 39(3), 425-437.

Omodei, M., Wearing, A., McLennan, J. (2000), “Relative efficacy of an open versus a restricted communication structure for command and control decision making: An experimental study”, In: C. McCann, R. Pigeau, Editors, “The human in command: Exploring the modern military experience”, Boston, MA: Springer US.

Pahnla, S., Siponen, M., Mahmood, A., (2007), “Employees' behavior towards IS security policy compliance”, 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), 56b-156b , Hyatt Regency Maui, HI, USA, 4–7 January.

Phillips, S. D., Friedlander, M. L., Pazienza, N. J., Kost, P. P., (1985). A factor analytic investigation of career decision-making styles. *Journal of Vocational Behavior*, 26(1), 106-115.

Radford, M. H., Nakane, Y., Ohta, Y., Mann, L., Kalucy, R. S., (1991). Decision making in clinically depressed patients: A transcultural social psychological study. *The Journal of Nervous and Mental Disease*, 179(12), 711-719.

Rhee, H.S., Kim, C., Ryu, Y. U., (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, 28, 816–826.

Rippetoe, P. A., Rogers, R. W., (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, 52(3), 596.

Rogers, R. W., (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114.

Rogers, R. W., (1983). "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation". In: J. T. Cacioppo, R. E. Petty, Editors, "Social Psychophysiology", New York, NY: Guilford.

Rowe, A. J., Boulgarides, J. D., (1992). "Managerial decision making: A guide to successful business decisions", New York: McMillan.

Rowe, A. J., Mason, R. O., (1987). "Managing with style: A guide to understanding, assessing, and improving decision making", Jossey-Bass.

Russ, F. A., McNeilly, K. M., Comer, J. M., (1996). Leadership, decision making and performance of sales managers: A multi-level approach. *Journal of Personal Selling & Sales Management*, 16(3), 1-15.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., Herawan, T., (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65–78.

Scott, S. G., Bruce, R. A., (1995). Decision-making style: The development and assessment of a new measure. *Educational and Psychological Measurement*, 55(5), 818-831.

Selart, M., Tvedt Johansen, S., Holmesland, T., Gronhaug, K. (2008). Can intuitive and analytical decision styles explain managers' evaluation of information technology?, *Management Decision*, 46(9), 1326-1341.

Singh, R., Greenhaus, J. H., (2004). The relation between career decision-making strategies and person–job fit: A study of job changers. *Journal of Vocational Behavior*, 64(1), 198-221.

Siponen, M., Pahnla, S., Mahmood, A., (2007). "Employees' adherence to information security policies: An empirical study". In: H. Venter, M. Eloff, L. Labuschagne, J. Eloff, R. von Solms, Editors, "New approaches for security, privacy and trust in complex environments", Vol. 232, Boston, MA: Springer.

Siponen, M., Mahmood, M. A., Pahnla, S., (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217-224.

Siponen, M., Vance, A., (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487–502.

Siponen, M., Vance, A., (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems*, 23(3), 289–305.

Stanton, J. M., Stam, K. R., Mastrangelo, P., Jolton, J., (2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), 124-133.

Sutton, J. C., (1982). Epidemiology of wheat head blight and maize ear rot caused by *Fusarium graminearum*. *Canadian Journal of Plant Pathology*, 4(2), 195-209.

Thunholm, P., (2004). Decision-making style: habit, style or both?. *Personality and Individual Differences*, 36(4), 931-944.

Tu, Z., Turel, O., Yuan, Y., Archer, N., (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, 52(4), 506-517.

Vance, A., Siponen, M., (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, 24(1), 21–41.

Vance, A., Siponen, M., Pahnla, S., (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3–4), 190–198.

Verizon, (2022).

<https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf> . Erişim Tarihi: 22.11.2023

Warkentin, M., Johnston, A. C., Shropshire, J., Barnett, W. D., (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 92, 25-35.

Westland, J.C., (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications*, 9(6), 476-487.

Woon, I., Tan, G. W., Low, R., (2005), “A protection motivation theory approach to home wireless security”, ICIS 2005 Proceedings31, Caen, France, 12–16 September.

Workman, M., Bommer, W. H., Straub, D., (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799-2816.

Youn, S., (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86-110.

ÖZGEÇMİŞ

Ahmet Düzensci, ilk ve orta öğrenimini Kırıkkale’de, lise öğrenimini Bursa’da bulunan Işıklar Askeri Lisesi’nde tamamlamıştır. Kara Harp Okulu Sistem Mühendisliği ve Anadolu Üniversitesi İktisat bölümlerinden Lisans derecelerini, Ege Üniversitesi Lojistik Yönetimi bölümünden Yüksek Lisans derecesini almaya hak kazanmıştır. Siber güvenlik alanında bir kamu kurumunda çalışmakta olup 2017 yılında Gebze Teknik Üniversitesi’nde Doktora eğitimine başlamıştır. Aynı zamanda Marmara Üniversitesi Fen Bilimleri Enstitüsü Siber Güvenlik Anabilim Dalı Başkanlığı akademik kadrosunda “Sızma Testleri ve Güvenlik Denetlemeleri” ve “Siber Savunma Teknikleri ve Kontrol Mekanizmaları” dersleri vermekte olan Düzensci’nin araştırma alanlarını; siber güvenlik yönetimi, siber güvenlik davranışı, siber güvenlikte yapay zekâ ve davranışsal araştırma konuları oluşturmaktadır.



TEZ ÇALIŞMASI KAPSAMINDA YAPILAN YAYINLAR

Duzenci, A., Kitapci, H., Gok, M. S., (2023). The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior. *Applied Sciences (Switzerland)*, 13(15), 8731.



EKLER

Ek-A: Kullanılan Ölçekler

<i>Boyutlar-İfadeler</i>	
<i>Algılanan Önem Derecesi</i>	
PeSe-1	Şüpheli bir e-posta ekini açmanın bir sonucu olarak bilgisayarına virüs bulaşması benim için ciddi bir sorundur.
PeSe-2	İş yerinde, gizli bilgilerime birisinin iznim veya bilgim olmadan erişmesi benim için ciddi bir sorundur.
PeSe-3	Bilgisayar korsanlığından kaynaklanan veri kaybı benim için ciddi bir sorundur.
PeSe-4	Çevrimiçi kimliğimin sosyal ağ siteleri aracılığıyla çalınması benim için ciddi bir sorun olur.
<i>Algılanan Savunmasızlık</i>	
PeVu-1	Bilgi güvenliği politikasına uymazsam kuruluşumun güvenlik ihlallerine açık hale gelebileceğini hissediyorum.
PeVu-2	Kuruluşumun bilgi güvenliği politikasına uymazsam kötü niyetli bir saldırının kurbanı olabileceğimi hissediyorum.
PeVu-3	Kuruluşumun bilgilerini koruma çabamın bunlara yasa dışı erişimi azaltacağına inanırım.
PeVu-4	Bilgi güvenliği politikalarına ve yönergelerine yeterince dikkat etmezsem kuruluşumun verileri ve kaynakları tehlikeye girebilir.
<i>Öz Yeterlik</i>	
SEfe-1	Web tarayıcısını farklı güvenlik düzeylerine ayarlamak konusunda kendime güvenirim.
SEfe-2	Bilgilerimi ve bilgi sistemimi korumak için farklı programlar kullanmak konusunda kendime güvenirim.
SEfe-3	Virüs bulaşmış dosyaları temizlemek ve/veya kötü amaçlı/casus yazılımlardan kurtulmak konusunda kendime güvenirim.
SEfe-4	Bilgi ve bilgi sistemimi koruma yöntemini öğrenmek konusunda kendime güvenirim.
<i>Yanıt Etkinliği</i>	
REfe-1	Kuruluşumdaki bilgi güvenliği politikalarına uymak, güvenlik ihlallerini düşük tutacaktır.
REfe-2	Bilgi güvenliği politikalarına uyarsam, bilgi güvenliği ihlallerinin oluşma ihtimali azalacaktır.
REfe-3	Bilgi güvenliği politikalarına dikkatle uymak, güvenlik sorunlarını önlemeye yardımcı olur.
REfe-4	Bilgi güvenliği teknolojilerini kullanmak, gizli bilgileri korumanın etkili bir yoludur.

<i>Algılanan Engel</i>	
PeBa-1	Eki olan bir e-postanın güvenliğini kontrol etmek zahmetlidir.
PeBa-2	Sosyal medya sitelerindeki gizlilik ayarını değiştirmek zahmetlidir.
PeBa-3	Bir bilgisayarı düzenli olarak yedeklemek zahmetlidir.
PeBa-4	Siber güvenlik eğitimi iş vaktinden çok fazla zaman alır.
<i>Güvenlik Farkındalığı</i>	
SeAw-1	Genel olarak, potansiyel bilgi/siber güvenlik tehditlerinin ve bunların olumsuz sonuçlarının farkındayım.
SeAw-2	Bilgi/siber güvenlik tehditleri ve genel olarak oluşturdukları risklerle ilgili endişeleri anlıyorum.
SeAw-3	Potansiyel bilgi/siber güvenlik tehditlerinin maliyeti hakkında yeterli bilgiye sahibim.
<i>Siber Güvenlik Uyum Davranışı</i>	
CCB-1	Tanımadığım kişilerden gelen e-posta eklerini açmam.
CCB-2	Şahsi bilgilerimi internet ortamında paylaşmam.
CCB-3	Yalnızca güvendiğim web sitelerini ziyaret ederim.
CCB-4	Yalnızca güvendiğim, tıkladığımda nereye gideceğimi bildiğim URL(adres)lere girerim.

Ek-B: Etik Uygunluk Kararı

Evrak Tarih ve Sayısı: 29.08.2022-70530



T.C.
GEBZE TEKNİK ÜNİVERSİTESİ REKTÖRLÜĞÜ
İnsan Araştırmaları Etik Kurulu

Sayı : E-43633178-199-70530
Konu : İnsan Araştırmaları Etik Kurulu
(Ahmet DÜZENCİ)

29.08.2022

Sayın Ahmet DÜZENCİ

İlgi : 03.08.2022 tarihli ve E.68423 sayılı yazınız.

İlgi yazıya istinaden yapmış olduğunuz başvuru, Üniversitemiz İnsan Araştırmaları Etik Kurulu'nun 17.08.2022 tarih ve 2022/12-02 oturum sayılı toplantısında incelenmiş ve değerlendirilmiştir. "Dijital Dünyada Siber Güvenlik Davranışı" konulu araştırma kapsamında kullanacağınız belgelerin etik açısından bir sakıncası olmamakla birlikte, tarafınıza iletilen bu yazıyı "Etik Uygunluk" belgesi niteliğinde değerlendirmenizi rica ederim.

Prof.Dr. Hüseyin İNCE
Başkan

Ek:İnsan Araştırmaları Etik Kurulu (1 Adet)

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Doğrulama Kodu :BSM4LMHRT2 Pin Kodu :72182

Belge Takip Adresi : <https://turkiye.gov.tr/ebd?eK=5466&eD=BSM4LMHRT2&eS=70530>

Adres:GEBZE TEKNİK ÜNİVERSİTESİ, İnsan Araştırmaları Etik Kurulu, 41400,
Gebze/KOCAELİ
Telefon:+90 262 605 (10 00) Faks:+90 262 653 84 90
Elektronik Ağ:www.gtu.edu.tr

Bilgi için: Seçil CALAP
Unvanı: Raportör

Tel No: 90 262 605 10 50



	T.C. GEBZE TEKNİK ÜNİVERSİTESİ İNSAN ARAŞTIRMALARI ETİK KURULU KARARLARI
Oturum Tarihi: 17.08.2022	Oturum Sayısı: 2022/12

KARAR:12-02) Üniversitemiz Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı İşletme Doktora Programı öğrencisi Ahmet DÜZENCI'nın 03.08.2022 tarihli ve E.68423 sayılı başvurusu görüşüldü ve aşağıdaki şekilde değerlendirildi.

Başvuru Tarihi:	03.08.2022
Protokol Sıra No:	12-01
Sorumlu Araştırmacıların Adı:	Ahmet DÜZENCI
Çalıştığı Birim:	Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı
Proje Çalışmasının Adı:	"Dijital Dünyada Siber Güvenlik Davranışı"
Toplantı Tarihi ve Oturum Sayısı:	17.08.2022 – 2022/12-02
Değerlendirme:	

Araştırmanın Amacı:	
Bireylerin karar verme tarzlarının siber güvenlik uyum davranışları üzerindeki etkisini incelemek.	
Araştırmanın Gerekçesi:	
Siber güvenlik alanında bireylerin içsel özelliklerinden olan karar verme tarzlarının siber güvenlik uyum davranışları üzerindeki etkilerinin tespit edilmesi sonucunda, hangi karar verme tarzlarına sahip bireylerin nasıl bir siber güvenlik uyum ya da uyumsuzluk davranışı göstereceğinin tespiti edilmesi amaçlanmaktadır.	
Araştırmanın Yöntemi:	
Araştırma modelini test etmek için anket metodolojisi kullanılacaktır. Anket, yayınlanmış literatürden çok maddeli ölçekler kullanılarak tasarlanmıştır.	
Çalışmaya Katılacak İnsanlarda Aranacak Özellikler:	
Çalışmanın katılımcılarının kamu ve özel sektör çalışanları ile iş tecrübesine sahip öğrenciler olması planlanmaktadır.	
Kullanılacak Psikolojik ve Teknik Yöntemler:	
Veriler, çalışanların siber güvenlik davranışları ile karar verme tarzları arasındaki ilişkileri değerlendirmek için bir anket aracı kullanılarak toplanacaktır. Çeşitli bölgelerden, kurumlardan ve demografiden veri toplamak için çevrimiçi anket yöntemi benimsenmiştir.	
Etik Özet:	
Katılımcılara verdikleri yanıtların anonim olarak saklanacağı konusunda bilgi verilecektir.	
Proje Yöneticisi: Ahmet DÜZENCI- Prof. Dr. Hakan KİTAPÇI	
Proje Araştırmacısı: -	
Projenin Yönetileceği Kuruluş: -	
Olası Tehlikeleri: -	
Araştırmanın nasıl finanse edileceği / Finanse eden kurum:	
Araştırma Bütçesi: -	
İnsan Araştırmaları için kullanılacak tutar: -	
K A R A R	
Kurul Üyelerinin bu çalışma ile ilişkisinin olup olmadığı incelenmiş olup, Kurul üyelerinin bu çalışma ile ilgili bir bağlantısı olmadığı görülmüştür.	

	T.C. GEBZE TEKNİK ÜNİVERSİTESİ İNSAN ARAŞTIRMALARI ETİK KURULU KARARLARI
Oturum Tarihi: 17.08.2022	Oturum Sayısı: 2022/12

KARAR:12-02) Üniversitemiz Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı İşletme Doktora Programı öğrencisi Ahmet DÜZENCI'nın 03.08.2022 tarihli ve E.68423 sayılı başvurusu görüşüldü ve aşağıdaki şekilde değerlendirildi.

Başvuru Tarihi:	03.08.2022
Protokol Sıra No:	12-01
Sorumlu Araştırmacıların Adı:	Ahmet DÜZENCI
Çalıştığı Birim:	Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı
Proje Çalışmasının Adı:	"Dijital Dünyada Siber Güvenlik Davranışı"
Toplantı Tarihi ve Oturum Sayısı:	17.08.2022 – 2022/12-02
Değerlendirme:	

Araştırmanın Amacı:	
Bireylerin karar verme tarzlarının siber güvenlik uyum davranışları üzerindeki etkisini incelemek.	
Araştırmanın Gerekçesi:	
Siber güvenlik alanında bireylerin içsel özelliklerinden olan karar verme tarzlarının siber güvenlik uyum davranışları üzerindeki etkilerinin tespit edilmesi sonucunda, hangi karar verme tarzlarına sahip bireylerin nasıl bir siber güvenlik uyum ya da uyumsuzluk davranışı göstereceğinin tespiti edilmesi amaçlanmaktadır.	
Araştırmanın Yöntemi:	
Araştırma modelini test etmek için anket metodolojisi kullanılacaktır. Anket, yayınlanmış literatürden çok maddeli ölçekler kullanılarak tasarlanmıştır.	
Çalışmaya Katılacak İnsanlarda Aranacak Özellikler:	
Çalışmanın katılımcılarının kamu ve özel sektör çalışanları ile iş tecrübesine sahip öğrenciler olması planlanmaktadır.	
Kullanılacak Psikolojik ve Teknik Yöntemler:	
Veriler, çalışanların siber güvenlik davranışları ile karar verme tarzları arasındaki ilişkileri değerlendirmek için bir anket aracı kullanılarak toplanacaktır. Çeşitli bölgelerden, kurumlardan ve demografiden veri toplamak için çevrimiçi anket yöntemi benimsenmiştir.	
Etik Özet:	
Katılımcılara verdikleri yanıtların anonim olarak saklanacağı konusunda bilgi verilecektir.	
Proje Yöneticisi: Ahmet DÜZENCI- Prof. Dr. Hakan KİTAPÇI	
Proje Araştırmacısı: -	
Projenin Yönetileceği Kuruluş: -	
Olası Tehlikeleri: -	
Araştırmanın nasıl finanse edileceği / Finanse eden kurum:	
Araştırma Bütçesi: -	
İnsan Araştırmaları için kullanılacak tutar: -	
K A R A R	
Kurul Üyelerinin bu çalışma ile ilişkisinin olup olmadığı incelenmiş olup, Kurul üyelerinin bu çalışma ile ilgili bir bağlantısı olmadığı görülmüştür.	